INVITATION FOR EXPRESSIONS OF INTEREST TO BE DESIGNATED AS A QUALIFIED LOCKBOX PROVIDER FOR FEDERAL AGENCY GENERAL LOCKBOX COLLECTIONS

Issue Date: August 15, 2003
Deadline for Submission of Notice of Intention to Respond: September 5, 2003
Deadline for Submission of Proposals: October 8, 2003

A Message from Assistant Commissioner Bettsy H. Lane

For 20 years, the Financial Management Service (FMS), a bureau of the U.S. Department of the Treasury, has been in the business of issuing solicitations for lockbox services and subsequently designating financial institutions as our agents. FMS wants and expects to be on the cutting edge in this business and in our other collections business lines. If your financial institution encourages innovation, we are interested in receiving a proposal for the lockbox services described in this solicitation.

Based on our 20 years of experience in the lockbox arena, we understand well that developing a response to this solicitation is a significant undertaking on your part. Your management will ask you for some level of assurance that their non-refundable investment in developing a proposal will eventually result in a sound return. While we obviously cannot guarantee that your proposal will result in your authorization to provide lockbox services, we know that with a strong commitment from the top of an organization and an innovative operational team, this business has proven profitable. Your role in processing a portion of the $26 billion collected through 277 general lockbox accounts for nearly 30 different Federal agencies can bring positive results to your bottom line and give you an edge in promoting your product lines with other customers in the public and private sectors.

For those of you considering a proposal, we are pleased to share with you some background on our lockbox program and where we envision the program going in the near future so that you may decide whether this business is a good fit with your organization's direction and goals. We'll start with explaining the uniqueness of this business line and then describe where we are headed in the next few years.

This Really is Different

For FMS, the lockbox business line is unique and challenging to administer. We have learned some important lessons in 20 years and want you to benefit from our experience.

FMS' Role

Years ago, we decided that the best way to manage the lockbox business was to separate out lockbox services for the Internal Revenue Service (IRS) from lockbox services for the rest of the Federal agencies. We did this because requirements for the IRS are unique within the Federal sector. We call our two lockbox business lines the IRS Lockbox Network and the General (read "non-IRS") Lockbox Network. The solicitation you are reading now exclusively involves the collection of non-tax payments and remittances received in **paper form** at the lockbox. Fedwire and Automated Clearing House (ACH) transactions will not be processed in the new network. The new network will further the government's adoption of 21st Century collection processes by utilizing flexible Web-based information flows and emerging technologies to expedite the collection and settlement of paper remittances received at designated lockboxes. We continue to examine even better ways to manage this business, and you will see a significant change in that

regard later in the document with your ability to bid on one, two, or all three types of general lockbox applications called retail lockbox, wholesale lockbox, and specialized wholesale lockbox applications.

In short, our role is to conduct this solicitation process and have it result in the establishment of a "schedule" of high-performing service providers from which to choose, to serve dozens of agencies, many of which have multiple bureaus deeper within their organizations. Consider FMS as the principal in assuring that: (1) the right service provider is matched with the right Federal program agency; (2) performance is up to specified standards; and (3) the Federal program agency is meeting its obligations for timely and efficient implementation and operation of the program.

The Lockbox Bank's Role

Banks that provide lockbox services to the Federal government have often told us that this business is a "one of a kind." Many banks try to find a "fit" for the Federal lockbox business within their existing corporate structure and come to realize that it deserves a unique position within their organization. For example, some banks have tried to couple this line of business with their "large corporate" customers, and soon realize that the profile of our business is quite different. Some banks have formed a separate "Federal government" sector, concentrating exclusively on serving their Federal customers. While it is not our place to dictate how you would manage this business, please accept as guidance that it deserves a unique approach.

When we designate a financial institution to provide lockbox services, the FI's staff becomes an extension of our workforce. They become our operational eyes and ears within the agencies, and we think of them as "one of us" – not free agents. We expect to have a very close partnership with our lockbox banks, so that we know what you know in real time. This is absolutely vital to the success of the program. While some of your customers may prefer an "arm's length" relationship with you, we seek the exact opposite. For example, in instances of urgent matters that may impact the security of our deposits, we will want direct access to your senior level officials, and expect that they will receive our phone calls at any time. We view this as a proactive and positive approach to doing business, and will expect that you share this same view.

Federal Agencies' Role

We work closely with Federal program agencies to determine their needs and to provide the best possible level of service to manage their collections.

The fact that we pay for the basic lockbox services provided to them (while they pick up the tab for what are called ancillary services) is certainly viewed favorably by them and by their budget examiners. The real challenge, in their view, is securing the commitment of us and of the lockbox banks to get to know their mission and their people. Federal program agencies are directed by Congress to implement laws and regulations related to their agency missions – they are not driven exclusively by financial management objectives as we are. Therefore, the "relationship" between FMS, the lockbox banks, and the agency is vitally important to the

success of the operations. We are all linked inextricably in assuring the success of the agency's mission by virtue of our ties to their collection operations. Your commitment to relationship management cannot be emphasized strongly enough as you contemplate responding to this solicitation.

All that said, we expect to create the most innovative and high-quality General Lockbox Network (GLN) possible on the cutting edge in agency collection processing. If that appeals to your organization, please read on.

A "Sea Change" is Coming

As we move forward with developing and utilizing new technologies, the paper lockbox program will change considerably from, in some cases, manual and partially automated processing and stovepipe system development and reporting, to a future paper lockbox which will offer electronic options for settlement and check clearing as well as centralized reporting and single system platforms. We will be embracing and implementing technological changes in lockbox as they become available in the marketplace. In some cases, we are pushing the industry to bring innovations to market as evidenced by the specifications within this solicitation. Even those lockbox banks with whom we have been partnering for up to 20 years will notice that this document is promoting a "sea change" in the way we process lockbox transactions. While incumbency may sometimes provide a level of familiarity with current business, the scope of changes we seek in operating the General Lockbox Network means that only the most creative, innovative, and cost-effective candidates will be certified at the end of the selection process. All responses, whether submitted by incumbents or non-incumbents, shall be evaluated objectively under the same standards.

To give you a flavor for these numerous changes, we would like to summarize them before you move into the main portion of this document.

Developing a Schedule of Service Providers

In previous solicitations for lockbox services, we designated financial institutions to perform lockbox services for specific Federal program agencies. In other words, at the end of the solicitation process, banks and agencies were teamed up for 5 or more years. With this solicitation, we will be certifying financial institutions to be what we call Qualified Lockbox Providers (QLPs). This certification process is referred to throughout this document as Phase I. In the ensuing months and years, we will be pairing the QLPs with the appropriate Federal program agency (called Phase II throughout the document) for specific cash flows.

This approach will provide maximum flexibility to all stakeholders. We will work closely with the QLPs and with the Federal program agencies to assure a good fit. For some applications, we will seek bids from QLPs, resulting in the designation being made of the QLP that provides the optimal response. In other cases, we will simply designate a QLP to perform lockbox services without seeking bids.

In Phase I of this solicitation, an FI will provide pricing for designated TMA codes. This pricing will be used as a cap for the initial term of the agreement. As indicated above, QLPs may have an opportunity to bid on specific lockbox accounts in Phase II. It is expected that the Phase II competition may lower these prices even further.

Three Types of Lockbox Business Lines

It has become very clear to us that there is not a "one size fits all" approach that works in serving Federal program agencies, and it is equally clear that some financial institutions specialize in providing cash management services.

Federal program agencies' missions and geographic reach are diverse. Some lockbox accounts have "typical remitter profiles" and others do not. Some accounts are great candidates for high-volume processing equipment, and others are not. Conversely, some financial institutions specialize in the plain vanilla retail applications and others prefer the more complex wholesale applications.

Therefore, we have created three different categories of lockbox services – retail, wholesale, and specialized wholesale. While the first two categories are self-explanatory, the third reflects that some agency specifications are especially complex. For example, the application process to obtain a U.S. Passport through the State Department requires considerable supporting documentation from the applicant and very secure handling by a QLP.

This differentiation process for the three types of accounts will require your careful consideration in deciding the category – one, two, or all three – in which to respond. The end result of this process will be a certified list of QLPs in each of the three categories, from which we will work with Federal program agencies to select the most appropriate service provider.

A Regional Approach

In this IEI, we are implementing a regional concept that has proven successful in the IRS Lockbox Network. For the first time in the General Lockbox Network, financial institutions will indicate in their proposal the region(s) of the United States in which they would provide lockbox services to Federal program agencies. By doing so, we recognize that financial institutions' footprints tend to be regional, capitalizing on their existing niche markets, and we will have yet another tool to best match a QLP with an agency's lockbox cash flow. We would discourage, though not prohibit, financial institutions from creating a lockbox site in a regional market they do not currently serve for purposes of enhancing their chances of becoming certified as a QLP. The lockbox product is a mature one, and we doubt that a financial institution would achieve internal support to build a new regional base, and we question whether a financial institution could be competitive if "new market" expenses had to be built into their cost proposals.

Security in a Changed World

Obviously, security requirements, including physical, personnel and information systems within this document have been strengthened since our last solicitation for general lockbox services back in 1994. The security of government receipts is our top priority and reflected in our specifications. We realize that some of the requirements may be more stringent than any of you have seen. We cannot compromise on any of them, and understand that they may hinder some otherwise very qualified service providers from submitting a proposal.

Nevertheless, this is an area in which we may be setting the trend for the private sector's handling of their secure documents and receipts. Our specifications will probably be showing up in future Requests for Proposals from your other potential public and private sector customers. Therefore, it may be in your best interest to review how to cost-effectively implement these security measures now, so that your organization remains competitive in the cash management arena.

Previous Performance

In this IEI, we will be examining the past performance of potential QLPs very vigorously. Again, all of our collections business lines, including lockbox, are now high profile, and we will ensure that the taxpayers are served by the highest quality service providers possible. For example, we welcome proposals from organizations that have implemented quality improvement and control programs.

Compensation of QLPs

Recently, we introduced a new method of compensation called the Depositary Compensation Security (DCS), which is a non-marketable security issued by the U.S. Treasury, the interest from which serves as payment to the service provider. This is a major step forward in opening the field of potential QLPs to more small and mid-size financial institutions because it eliminates the requirement to collateralize large compensating balances. We have been told over the years that collateralization requirements for compensating balances were show-stoppers for some potential service providers, and we will continue to explore options that will ease any administrative burdens in this area and enhance competition. As part of this network, however, FMS may compensate QLPs via any of the following options, at FMS' sole discretion: Compensating Balances, Depositary Compensation Securities, Direct Payments via ACH, and any other method, which may become available.

Technological Advances – Macro

In the past 3 years, FMS has been developing several initiatives intended to incorporate the latest technological advances in information and collections processing. All of these will impact how QLPs serve Federal program agencies in the coming years and will require maximum flexibility on all stakeholders' parts as they are implemented initially and in updated versions.

First, FMS has created and implemented a product called Pay.gov that enables Federal program agencies' receipt of funds and transmission of data via Web-based technology. The Federal Reserve has been designated as the lead in rolling out this program Governmentwide, and designated QLPs can expect to work closely with them on cross cutting measures. One measure will include the Internet matching of checks received in the lockbox with electronic forms processed by Pay.gov.

Additionally, our current lockbox network includes "electronic lockbox accounts" through which we collect Automated Clearing House (ACH) and Fedwire transactions. All of these accounts will be closed over the next year and we will begin processing these electronic collections through Pay.gov. With this change, funds will be settled by the Federal Reserve directly into Treasury's account instead of passing through a QLP. Until this conversion is completed, current service providers will continue to process the "electronic lockbox accounts" under existing arrangements. As a result, this General Lockbox Network (GLN) will only process paper check transactions.

Also, FMS will be implementing shortly a new and improved internet-based cash concentration and reporting system called CA$HLINK II. All deposits received via lockbox will be reported into CA$HLINK II. Monthly account analysis statements will also be submitted through CA$HLINK II.

And finally, FMS is developing a Central Reporting System (CRS) that will, among other things, provide Federal program agencies with a single, consolidated daily report of all revenue activity across all collection systems. Once this is implemented, QLPs will be required to interface with it and should realize substantial operational efficiencies.

Technological Advances – Micro

When we began processing collections via lockbox 20 years ago, the primary cost-savings came from speeding the flow of funds into the Treasury to take advantage of the high percent interest rates that prevailed. Every day delayed in depositing funds had a profound impact on our cash position. Now, 20 years later and with interest rates at historic lows, we have mastered the speedy deposit of funds and have turned our attention to saving costs by using the most modern technology possible.

This IEI is seeking proposals that will implement cost-cutting measures like imaging technology, check truncation, paper check conversion (PCC), and linking credit card collections to the lockbox processing operations, just to name a few. Of particular note, the introduction of PCC in lockbox processing will require QLPs to separate items for settlement. Convertible items processed via PCC will be settled by the Federal Reserve; non-convertible items will be settled by the QLP. Additionally, QLPs will be expected to interface with the Imaging Enterprise Platform that will be built according to the proposal outlined in the Technical Requirements of the IEI. While some debate ensues regarding the appropriate means to implement these measures, there is no debate over whether we want to move ahead on these fronts. We are serious about reaching the goal of processing 100 percent of our collections electronically, and

see these products as tools to get from the current 80 percent electronic collections rate to 100 percent.

Summary

We hope that this introductory message has been helpful in describing where we want to take the General Lockbox Network. Be assured that there is time allotted in this process for you to ask questions about this document and to receive answers timely so that you can meet the deadlines for submitting proposals. We thank you in advance for your interest in our program and look forward to hearing from you.

Bettsy H. Lane
Assistant Commissioner
Federal Finance

August 15, 2003

GENERAL LOCKBOX NETWORK
INVITATION FOR EXPRESSIONS OF INTEREST
TABLE OF CONTENTS

1.0 INTRODUCTION

The Financial Management Service (FMS) is pleased to issue this General Lockbox Network (GLN) Invitation for Expressions of Interest (IEI) to all qualified financial institutions. In order to help you navigate through this document, below is a snapshot of the upcoming sections in this IEI, along with key features of the new GLN (pay close attention to the Technical Requirements section).

> **Section 2.0 Administrative Aspects and Threshold Requirements** outlines the threshold requirements to participate in the IEI competition and how FMS will administer the GLN.
>
> **Section 3.0 Response Requirements** describes the processes necessary to respond to the IEI, and includes deadlines, criteria and scoring elements, along with a map of the five geographic regions that are designated for servicing the GLN.
>
> **Section 4.0 Technical Requirements** specifies current, new and unique features, such as the Central Reporting System, CA$HLINK II, standardized Treasury Management Association (TMA) codes, Internet Check Matching via Pay.gov, Paper Check Conversion, Check Truncation and Disaster Recovery and Continuity Plans.

Four appendices follow the last section:

> **Appendix 1 – Legal Agreements – DFA and MOU** (models),
> **Appendix 2 – Technical Evaluation Criteria,**
> **Appendix 3 – Pricing Response Templates,**
> **Appendix 4 – Glossary of General Lockbox Terms.**

Throughout the IEI, several attachments are referenced and are available on FMS' Web site at www.fms.treas.gov/rebids/attachments.

Finally, the IEI, and its appendices and attachments, refer to the terms "financial institution", "Financial Agent" and "Qualified Lockbox Provider". In order for prospective bidders to understand these terms, we offer the following definitions:

> ***Financial Institution (FI)*** – An FI is a financial institution eligible under 31 CFR 202.2 to be designated by the Financial Management Service as a Financial Agent to provide various types of essential banking services.
>
> ***Financial Agent (FA)*** – An FA is an institution that is designated an agent by and enters into an agreement with the Financial Management Service, as principal, to provide various types of essential banking services.

Qualified Lockbox Provider (QLP) – A QLP is a designated Financial Agent that becomes a service provider within the General Lockbox Network. A QLP may bid on or be assigned business within the General Lockbox Network, depending on the availability and location of that business.

2.0 ADMINISTRATIVE ASPECTS AND THRESHOLD REQUIREMENTS

2.1 Designation of an FI - Phase I and Phase II

As mentioned in the opening message from the Assistant Commissioner of Federal Finance, this IEI presents a two-phased process; differentiates retail, wholesale, and specialized wholesale lockboxes; and, implements a regional approach – all to assure that the best possible lockbox services are provided for Federal program agencies.

Phase I encompasses the receipt, review, and evaluation of proposals from interested and qualified FIs. As part of this process, FIs will indicate the type of lockbox service they propose to provide (retail, wholesale, and/or specialized wholesale) and the region of the country in which they propose to provide this service (see Sections 3.5 and 3.6).

Phase I of this competitive process will culminate in the designation of FIs as Qualified Lockbox Providers (QLPs). It should be noted that designation, during Phase I, as a QLP does not guarantee any lockbox processing work or compensation during the term of the GLN.

Then, once the new GLN is underway later this year with its QLPs in place, Phase II will begin. Phase II will encompass the selection by FMS of designated QLPs to actually perform lockbox processing work for specific Federal agency cash flows. In Phase II, FMS may, depending on the specific Federal agency collection flow that needs to be processed:

1. Assign the work to an eligible QLP without further competition, if FMS determines, in its sole discretion, it is in the best interests of the Federal government to do so, or

2. Conduct a mini-competition among eligible QLPs in the pertinent Region to determine which QLP will be assigned the processing work.[1]

FIs designated as QLPs in a particular Region shall be required to perform specific lockbox processing work if directed by FMS to do so in Phase II, for an amount not to exceed the ceiling price. In addition, if FMS initiates a Phase II mini-competition in a particular Region, and no bids are received during Phase II from eligible QLPs in that Region, FMS reserves the right to either: a) direct any QLP in the Region to perform the work at the ceiling price, or b) assign the work to an out-of-region QLP or non-QLP. Thus, QLPs do not have the option of rejecting work assigned by FMS in Phase II. FMS anticipates that the outcome of Phase II competitions will be primarily determined by price considerations, although FMS reserves the right, in its sole discretion, to evaluate other objective factors, including, but not limited to availability, technical merit and past performance, as deemed appropriate, on a case-by-case basis.

[1] FMS also reserves the right to assign specific Federal agency collection flows to a non-QLP, or to an out-of-region QLP, if it believes it is in the best interests of the Federal government to do so, or if requested to do so, in writing, by the Federal agency for reasons that include, but are not limited to, maintaining the continuity of Federal agency operations, security concerns, or other exigent circumstances.

The pricing responses submitted by FIs in response to this IEI will operate as a ceiling in Phase II, i.e. QLPs assigned processing work by FMS in Phase II must perform required services at or below the prices specified in the FI's response to this IEI. QLPs bidding for a specific Federal agency collections flow in a Phase II competition will need to make a competitive business decision whether to submit the ceiling price or a lower price. Any bid submitted by a QLP in a Phase II competition above the ceiling price will not be considered. The following three examples illustrate, in part, the Phase II Selection Process:

GLN Phase II Selection Process Example #1 (Competitive Selection)

Federal Agency A requires wholesale lockbox services in Region 1. Three FIs were designated by FMS as QLPs in Region 1 for wholesale lockbox services at the conclusion of the IEI competition. FMS establishes Phase II competition criteria and thereafter administers a Phase II competition to determine which of these three QLPs will be awarded the work. All three QLPs eligible to perform wholesale work in Region 1 submit bids at prices at or below the ceiling amount. A fourth QLP only eligible to perform wholesale work in Region 2 requests permission to enter the Phase II competition. FMS rejects the request because the fourth QLP is not eligible to provide wholesale services in Region 1, and the circumstances referenced in IEI footnote 1, do not apply in this particular case. Based on the Phase II proposals submitted by the 3 eligible QLPs, FMS selects one of them to perform wholesale work in Region 1 for Federal Agency A based on an objective evaluation of the Phase II competition criteria.

GLN Phase II Selection Process Example #2 (Competitive Selection)

Federal Agency B requires retail lockbox services in Region 3. Two FIs were designated by FMS as QLPs in Region 3 for retail lockbox services at the conclusion of the IEI competition. FMS determines that it will conduct a Phase II competition for this Federal Agency collection flow but neither of the eligible QLPs responds to FMS' request for Phase II bids. FMS may: a) direct either of the two QLPs in the Region to perform the work at the ceiling price provided in Phase I (in which case the selected QLP may not decline the work), or b) assign an out-of-region or non-QLP financial institution to perform the work.

GLN Phase II Selection Process Example #3 (Non-competitive Selection)

Federal Agency C requires retail lockbox services in Region 5. Federal Agency C has a large collection flow that requires significant oversight by Agency personnel. Federal Agency C worked with QLP #1 in the former GLN and wants to continue the relationship with QLP #1 because any switch in lockbox banks providing retail lockbox services will require an inordinate expenditure of time and resources by Agency C to maintain the continuity of Federal agency operations. Federal Agency C submits a written request for FMS to extend QLP #1's authority to continue processing the collection without a Phase II competition. QLP #1 has not been designated as a QLP in Region 5, but is a designated QLP in another Region. FMS agrees with the written request and selects QLP #1 as the lockbox bank without conducting a Phase II competition. Agency C may be required to absorb the additional costs for QLP #1 to perform the work for Federal Agency C if the costs are higher than for the QLPs in Region 5.

2.2 Eligibility to Participate in the IEI Competition

All FIs that are qualified to be designated as depositaries and financial agents of the United States under 31 Code of Federal Regulations (CFR) Part 202 (see http://www.access.gpo.gov/nara/cfr), and that otherwise meet the threshold requirements under IEI, Section 2.6 are eligible to participate in this IEI competition. Responses submitted by entities that do not meet these requirements will not be considered.

2.3 Authority to Designate

Pursuant to Sections 265 of Title 12, United States Code (U.S.C.), 31 U.S.C. Chapter 33, 31 CFR Part 202, and other authorities (see e.g., 12 U.S.C. §§ 90, 266, 1464(k), and1789a), the Secretary of the Treasury has authority to designate FIs to be depositaries and financial agents of the United States. The Secretary of the Treasury has delegated to FMS the authority to select and designate depositaries and financial agents for, among other purposes, lockbox collection services.

Depositaries and financial agents designated to perform lockbox services by FMS, as Principal, act in Treasury's stead for the stated purposes, a function that does not constitute a procurement within the meaning of the Federal Property and Administrative Services Act (41 U.S.C. §§ 251-260). Thus, this IEI is **not** a procurement subject to, or governed by, the Federal Property and Administrative Services Act or the Federal Acquisition Regulation (FAR). See e.g., United States v. Citizens & Southern National Bank, 889 F.2d 1067, 1069-70 (Fed. Cir. 1989).

2.4 Right to Amend IEI; Disclaimers

Information contained in this document is subject to modification to comply with legislative, regulatory, organizational, or policy changes. FMS may amend this IEI at any time prior to the selection of QLPs. If appropriated funds are used to pay for services under this IEI, the government's obligation is contingent upon the availability of appropriated funds from which payment for the agreed-upon services can be made. No legal liability on the part of the government for any payment may arise until funds are made available for the performance of banking services under this IEI. This IEI shall, in no way, commit the Federal government to any legal or fiduciary obligation to any of the respondents to this IEI.

FMS is not liable for any costs incurred by respondents in preparing and submitting a response to this IEI.

FMS reserves the right to accept or reject any and all responses, in whole or in part, received in response to this IEI, or to waive or permit the cure of minor irregularities to serve the best interests of the Federal government.

Based on the responses to this IEI, FMS may select and designate as QLPs those FIs whose response FMS determines, in its sole discretion, to be optimal in terms of evaluated point scores, and in the best interests of the Federal Government.

A responding FI may be required to provide additional information orally or in writing, or to submit to a site inspection by FMS representatives, in order to clarify or document the FI's responses and qualifications.

FMS may cancel this IEI, in whole or in part, whenever cancellation is determined to be fiscally advantageous to the Federal Government or otherwise in its best interest.

2.5 Public Information And Freedom of Information Act

All responses to this IEI and documents pertaining to the responses will be open to the public, except for material, which has been designated by responding FIs as proprietary or confidential. Pages containing such information shall be marked by FIs with the following statement: "This page contains confidential and proprietary information."

If a request under the FOIA is received for disclosure of proprietary or confidential data for which an FI has made a written request for confidentiality or otherwise designated information as commercially or financially sensitive, FMS will advise the FI of such request and provide the FI with the opportunity to provide a detailed statement within 10 working days specifying any objection to disclosure. Refer to 31 CFR 1.6(d) for specific objection requirements. FMS will evaluate any objection to disclosure and resolve the request for disclosure in accordance with 31 CFR 1.6(e).

2.6 Financial Agent Qualifications Under This IEI

The role of a QLP, as financial agent (FA), is to act on behalf of the U.S. Treasury in providing financial services to Federal departments and agencies. FMS is seeking to build a solid working relationship with the selected QLPs that benefits all parties and that evolves with new and proven technologies to result in increased efficiencies.

Responses shall be accepted from FIs meeting the qualifications of this section. Failure to meet any of the qualifications listed below shall result in the rejection of the response from further consideration. To be eligible to compete for selection as a QLP under this IEI an FI shall:

1. Be eligible to be designated as a depositary and financial agent of the United States as defined in Title 31 CFR Part 202;
2. Be in compliance with existing Treasury regulations and procedures concerning the handling of government deposits;
3. Not be on the Federal Debarment and/or Suspension List and not be delinquent on any debts owed to the U.S. Government;
4. Provide a response that demonstrates that the FI understands the technical and other requirements of this IEI and that it is completely responsive to those requirements;

5. Be able to perform all of the requirements of this IEI;
6. If currently doing business with FMS, not be in a probationary status, and has addressed and resolved any identified deficiencies in performance, if any;
7. Covenant that it shall address, to the satisfaction of FMS, any potential personnel or organizational conflicts of interest as between itself or any subsidiaries or contractors;
8. If currently doing business with FMS, have completed and submitted to FMS all required information in internal and external audits of depositary services currently required by Treasury;
9. Be able to partner with other FAs, when determined by FMS to be in the best interest of the government; and
10. Comply fully with all security requirements detailed in Section 4.0, Technical Requirements.

2.7 Compensation

The method of compensating a QLP for required general lockbox services is at the sole discretion of FMS. FMS may compensate the QLP by means of Depositary Compensation Securities (DCS), a compensating balance, direct payment, or other appropriate method. Whichever method of compensation is chosen, FMS will fully disclose to the QLP all terms, conditions, requirements, and obligations under that form of compensation.

The three potential methods of compensation available at this time are described as follows:

Compensating Balance is a balance placed at an FA in a Treasury Time Balance (TTB) account. Compensation is made through the imputed earnings on the investable balance using an earnings credit rate (ECR) provided by FMS. The investable balance includes a TTB held by the FA in a separate non-interest-bearing account expressly for this purpose and (where appropriate) collected balances from lockbox deposits.

Depositary Compensation Securities are non-marketable securities issued by the U.S. Treasury to FAs as an investment vehicle that will be used for investing funds maintained in the TTB account. Compensation is made by means of the interest accrued on these securities, which is paid to the FA on a monthly basis.

Direct Payment is a payment to the FA reimbursing it directly for banking services provided. This payment, either an Automated Clearing House (ACH) or Fedwire transaction, is made on a monthly basis.

This IEI does not guarantee any quantity or minimum amount of business or compensation to a QLP. Requirements set forth by FMS, which fail to result in the level of activity, or compensation anticipated by any party shall not constitute the basis for price adjustments or additional compensation to a QLP.

2.8 Agreements

The following agreements shall be executed at the times specified in this section.

2.8.1 Designation and Authorization of Financial Agent (DFA)

Upon selection as a QLP, the FI then shall execute the DFA with FMS (see Appendix 1 of this IEI). The DFA designates the FI as a lockbox depositary and financial agent of the United States and details the legal requirements, and principal/agent relationship between FMS and the QLP. The terms of the DFA are not negotiable. The duration of the DFA will be an initial term of three (3) years, with two (2) two-year renewal options that FMS has the sole discretion to exercise in whole or in part. The contents of this IEI and the responses submitted by an FI will be incorporated by reference into the DFA (see Appendix 1).

2.8.2 Memorandum of Understanding (MOU)

At the sole discretion of FMS, QLPs may bid for or be assigned Federal agency business during the Phase II selection process. A QLP awarded such Federal agency business shall execute an MOU with the Federal agency and FMS, detailing the agreement among the parties of the specific General Lockbox services to be performed (see Appendix 1 for a model MOU).

3.0 RESPONSE REQUIREMENTS

3.1 Written Responses

3.1.1 Notice of Intention to Respond

FIs interested in responding to this Invitation shall send a completed Notice of Intention to Respond Form. (The form required to be completed is provided in Attachment A on FMS' Web site at www.fms.treas.gov/rebids/attachments) to the FMS contact listed below by 4:00 p.m. (ET) no later than September 5, 2003.

Financial Management Service
Program Assistance Division
Attn: Carolyn Dunston, Program Manager
Room 415A
401 14th Street SW
Washington, DC 20227
Telephone: 1-800-487-1735
Facsimile Number: (202) 874-6965

The Notice may be sent by mail, fax, via hand delivery, or messenger service. Those FIs submitting the Notice by fax must follow up the fax transmission with a mailed copy of the original Form.

FIs that do not submit a completed Notice of Intention to Respond Form by September 5, 2003, ***will not*** be eligible to submit responses to this IEI.

The Notice, which shall be signed by an authorized FI official, requires the FI to certify that the FI meets the threshold requirements to participate in the IEI competition. It also requires the FI to submit, as references, the names of its top ten largest lockbox clients (based on transaction volume) by September 5, 2003. The FI submitting the Notice authorizes FMS to contact these references and to use the information collected for IEI competition evaluation purposes. For those FIs currently performing Federal agency lockbox work on behalf of FMS, at least four (4) of the references must be Federal agencies. For those FIs not currently performing Federal lockbox work on behalf of FMS, the FI is requested to provide client references from state or local government customers or large decentralized corporations. The Notice also requires the FI to specify its point of contact for the IEI competition.

Each Notice of Intention to Respond Form and all information provided by an FI will be held in complete confidence, subject to the provisions of Section 2.5.

The Notice of Intention to Respond Form specifies that an FI may elect to withdraw from the process at any time prior to the selection by FMS of QLPs. It is the expectation of FMS that an FI shall notify FMS in writing of such withdrawal.

3.1.2 Substantive Response Requirements and Point of Contact

FIs shall submit a written response addressing all the requirements of this IEI. The FI shall submit seven (7) copies of its written response. The written response shall consist of four (4) parts: a technical response, security certification, past performance response, and a price response. FIs shall also submit pricing responses on a diskette in Microsoft Excel format. Response requirements for each of these parts are addressed in Section 3.4. Technical responses shall provide a detailed description of how the FI plans to address all of the requirements described in this IEI. The technical responses shall not contain any price information. The security certification requirements are outlined in Section 3.4.5. Price responses shall contain all price information related to the services requested in this IEI, by TMA code and proposed lockbox processing site within a Region (see Section 3.4.4). The entire response must be submitted as a package and received no later than 1 p.m. (Eastern time) on October 8, 2003 at the address in Section 3.1.1.

Responses received after the time indicated ***will not*** be considered.

Responses may be mailed or hand-delivered**; FMS will not accept e-mail or fax responses**. All responses shall be signed by an officer of the FI authorized to make the commitments and representations included in its response. Responses to each section (technical, past performance, security, and pricing) shall be separately identified, sealed, and bound and sent in one delivery.

Written responses shall be evaluated in accordance with the criteria specified in this IEI.

3.2 IEI Clarifications/Questions

FMS' Point of Contact will accept written questions regarding this IEI (including the attachments and appendices) at any time up to September 5, 2003. E-mail questions to the following address: general.lockbox.rebid@fms.treas.gov. Questions shall be concise and cogent and must contain an IEI citation where applicable. All questions must also include an FI contact person and phone number in case FMS requires any further explanation. FMS' verbal responses shall not be legally binding. However, FMS' Point of Contact will answer and post all written questions timely submitted on the FMS Rebid Web site located at http://www.fms.treas.gov/rebids.

NOTE: It is not permissible for an FI, or any entity representing the FI, to request information from any governmental source other than from FMS' Point of Contact or her designee. Any violations regarding requests for information or attempts to contact Treasury personnel other than the designated Point of Contact or her designee concerning this IEI are grounds to disqualify the violator's response from consideration, thereby precluding the FI from participation in this IEI.

FMS intends to provide full and complete answers to properly submitted written questions in order to clarify pertinent IEI issues. FMS reserves the right to provide a single aggregated

response to questions submitted on the same or similar topics to avoid duplication and confusion. Amendments, if any, to this IEI resulting from written questions submitted in accordance with this section will be posted on FMS' Rebid Web site at www.fms.treas.gov/rebids. The Point of Contact for each FI who submitted a Notice of Intention to Respond letter will be automatically e-mailed with a notification that the FMS Rebid Web site has been updated with new information.

3.3 Schedule of Key Dates and Deliverables

IEI Activities	Date
Release of Invitation for Expressions of Interest	August 15, 2003
Notice of Intention to Respond Form/Past Performance References Due	September 5, 2003
Deadline for Submission of Written GLN Questions	September 5, 2003
Responses to GLN Questions Published	September 19, 2003
Written Responses to IEI Technical Requirements Due	October 8, 2003
Written Responses to IEI Pricing Proposal Due	October 8, 2003
Completed Financial Institution Questionnaire Due	October 8, 2003
Security Certification Due	October 8, 2003
Complete Evaluation of Responses	October 29, 2003
Announcement of FIs Selected As QLPs*	November 5, 2003
Signing of DFAs	November 21, 2003
On-Site Security Reviews of QLPs	November 2003 – January 2004
Security Deliverables	
Security Awareness Program	November 21, 2003
Facility Security Plan	November 21, 2003
Occupant Emergency Plan	November 21, 2003
Facility Blueprint A. Initial Facility Blueprint B. Final Facility Blueprint	 A. November 21, 2003 B. December 19, 2003
Continuity of Operations Plan	November 21, 2003
Completion of Security Awareness Training	December 31 , 2003

***Note:** Selections are contingent upon, and subject to, acceptable Security Documents, as well as certification of satisfactory Physical and Personnel security reviews conducted by FMS.

3.4 Contents of Proposal/Criteria and Scoring

3.4.1 Content and General Scoring Information

Interested FIs are required to prepare and submit seven copies of their proposal that is in compliance with the specifications shown in this section. Because each part will be evaluated by

a separate and distinct review panel, a proposal will consist of seven copies of four separately bound parts: 1) technical; 2) past performance; 3) pricing and 4) security.

All parts should be delivered in one package to FMS, with pricing proposals sealed securely within the single package.

More succinctly, banks should submit in one box/package: 1) seven copies of spiral bound technical proposals; 2) seven copies of bound security certifications; 3) seven copies of bound past performance proposals; and 4) seven copies of bound price proposals, each in a separate and secure envelope.

Specific security documents, including the Security Awareness Program, Facility Security Plan, Occupant Emergency Plan, Facility Blueprint, and Continuity of Operations Plan will be submitted at a later date in a separate package.

To assist you in preparing your proposal, each of the following sections contains bold print showing exactly what documents should be submitted by the financial institution.

Evaluation of Responses

Responses shall be evaluated in order to determine compliance with the mandatory requirements of this IEI, and to determine which responses are optimal in terms of technical requirements, past performance, pricing and security. Each technical, past performance, and pricing proposal will be awarded points during the evaluation process. Security requirements will be evaluated on a pass/fail basis.

During the evaluation process, FMS will award the following range of points: Technical Requirements Response (0-300), Past Performance Response (0-100), and Pricing (0-100). Thus, the maximum score possible for these three required categories is 500.

Technical Requirements (60%)	**Maximum Score = 300**
Staffing and Management Personnel	(0-45 points)
Mail Processing/Handling	(0-55 points)
Data Capture/Transmission	(0-60 points)
Disaster Recovery & Continuity Plans	(0-50 points)
Record Retention	(0-20 points)
Lockbox Processing	(0-70 points)
Past Performance (20%)	**Maximum Score = 100**
Performance Questionnaire for FIs	(0-20 points)
Client Questionnaire	(0-60 points)
Required Audit Information	(0-20 points)

Pricing (20%)	**Maximum Score = 100**
Security	**Pass/Fail**

In addition, FIs are encouraged, but not required, to submit proposed innovative ideas to improve the GLN. Approved innovations may result in the FI being awarded bonus points as described under IEI, Section 3.4.6.

Each separate response submitted by an FI will be awarded a distinct score.

> **Example:** Consistent with IEI Section 3.5, a particular FI submits responses to provide lockbox services in Region 1 (retail and wholesale), and Region 2 (wholesale and specialized wholesale), FMS will evaluate the responses as four separate submissions. Thus, the FI will receive four different evaluated scores: Region 1 retail, Region 1 wholesale, Region 2 wholesale, and Region 2 specialized wholesale.

Those FIs with the highest evaluated points will be designated QLPs by FMS in the pertinent Region(s), and in the pertinent service category: retail, wholesale, and/or specialized wholesale. As stated in IEI, Section 3.5, FMS intends to designate one or more QLPs in each Region in each lockbox sub-category: retail, wholesale, and specialized wholesale lockbox, based on evaluated score results.

Keep in mind that FMS evaluators may award a minimal number of points in the technical requirements category if the FI merely addresses pro forma the mandatory technical requirements in the IEI. FMS evaluators may award more points (not to exceed 300) if the technical response provides greater and more helpful detail, which demonstrates a better quality understanding and ability to meet the mandatory requirements.

3.4.2 Technical Proposal

Respondents will be rated on how well they propose meeting the technical requirements. Unless otherwise noted, all services described in this IEI are mandatory. For the convenience of FIs preparing proposals, FMS has listed at Appendix 2, the Technical Evaluation Criteria and topics to be considered during the Technical Response evaluation process.

As noted above, the technical proposal score (0-300) is worth 60% of the total evaluation score.

3.4.3 Past Performance Response

FMS is committed to providing Federal government agencies with the most effective and efficient general lockbox services available. To that end, FMS will take careful note of and rate all responding FIs past performance in their lockbox business line. FMS will evaluate the following items in order to determine a past performance score:

1. The completed **Performance Questionnaire for Financial Institutions**, submitted by FIs with their proposals (see IEI Attachment B on FMS' Web site: www.fms.treas.gov/rebids/attachments).

2. The **Client Questionnaire** responses from references supplied by the FI as required by Section 3.1.1. FMS will send client questionnaires to at least five (5) of the ten (10) references provided. FMS may also contact the clients by telephone.

3. **Required Audit Information.** Financial institutions shall provide the opinion letter from the independent auditor that performed the most recent SAS 70 audit evaluating the adequacy of controls of the FI's lockbox operations. If there are substantial weaknesses noted in the opinion letter, the FI shall provide a description of the actions taken to address the weaknesses. At the request of FMS, the FI may be required to provide the complete copy of the SAS 70 audit.

   Financial institutions that have not previously been required to have an SAS 70 audit conducted on their lockbox operations shall provide sufficient documentation that a review, which includes the lockbox operations, has been conducted within the past two years. This review can be a part of an internal or external review. The FI shall provide a description of actions taken to address significant weaknesses noted in such reviews. If selected, a QLP will be required to provide an independent audit of its lockbox operations using an SAS 70 Type II audit standard as described in the General Lockbox Processing Technical Requirements, 4.9 Audit and Report Requirements on the reporting schedule described therein.

As noted above, the past performance score (0-100) is worth 20% of the total evaluation score.

3.4.4 Pricing Response

Respondents must submit proposed pricing responses per TMA code, per proposed regional site and type of lockbox (retail, wholesale, and specialized wholesale) by completing the pricing response templates in the format provided in Appendix 3. Appendix 3 includes three Pricing Response templates: one for Retail lockbox services, one for Wholesale lockbox services, and one for Specialized Wholesale lockbox services. The FI must indicate on the top of each completed template the region to which the response applies.

> **Example:** If an FI is submitting proposals to provide lockbox services in Region 3 (retail and wholesale), and Region 4 (retail and wholesale), the FI must submit four separate pricing response templates: two separate retail lockbox pricing templates marked Region 3 and Region 4, respectively, and two wholesale lockbox pricing templates marked Region 3 and Region 4, respectively.

Please note that the three pricing templates (retail, wholesale, and specialized wholesale) provided at Appendix 3 each have a volume figure associated with the TMA codes. These volumes were derived by taking the most recently available aggregate nationwide lockbox

volumes (for each type of lockbox) and dividing that figure by 5, to reflect the new regional approach. Thus, these volumes are provided for evaluation purposes only. The template volumes do not reflect projections for future business, nor are they intended to reflect actual current business activity because the regional approach is new and actual weighted figures for regions are not yet available. FIs submitting responses to this IEI expressly acknowledge, without recourse, that volumes short of the numbers provided in any template, in any region (or regions in the aggregate), during the term of the new GLN will not provide grounds for an upward price adjustment in any case at any time. Volumes of business and levels of compensation are not guaranteed.

For the convenience of FIs submitting proposals, FMS has provided under IEI, Section 3.5 information on the states presently assigned to the five distinct regions.

FMS has decided that in the new GLN, all costs associated with post office box rentals and courier related services will be treated as a "Pass-Through", i.e., FMS will compensate the bank its reasonable actual cost for these services (no mark-up), provided FMS approves, in advance, the amount of the Pass-Through charge.

FMS will not be soliciting Best and Final Offers in Phase I, so respondents are encouraged to submit bids with their best prices. FMS is seeking the same or better discounts as the respondents provide to their best corporate, state, or local government customers.

As noted above, the pricing proposal score (0-100) is worth 20% of the total evaluation score.

Note: Pricing will be fixed for 3 years, with two two-year options to renew thereafter. At each renewal, the price adjustment for the option period may not exceed the lesser of either: (a) the **Consumer Price Index (CPI)**, specifically entitled the *CPI-U, U.S., All-items (not seasonally adjusted)*, or (b) the **Employment Cost Index (ECI)**, specifically entitled the *ECI for Total Compensation (not seasonally adjusted), private industry workers, white collar, administrative support including clerical occupations*. Regardless of the CPI or ECI index, in no case shall the price adjustment for the option period exceed 4.9 percent (the average change in the *CPI-U, U.S., All items index (not seasonally adjusted)* between 1970 and 2002).

The Bureau of Labor Statistics produces the CPI and ECI. The CPI and ECI consist of various indexes based on population coverage, geographic region, item or occupation coverage, and seasonality. The *CPI-U, U.S., All-items index (not seasonally adjusted)* is the CPI-All Urban Consumers for the United States (approximately 87 percent of the total U.S. population). It covers expenditures on all items purchased by families living in urban areas and is not adjusted for seasonal expenditure patterns. It represents about 87 percent of the total U.S. population and is based on the expenditures of all families living in urban areas. The *ECI for Total compensation (not seasonally adjusted), private industry workers, white collar, administrative support including clerical occupations* shows changes in total labor costs for a specific type of worker in a specific occupational group. This index is also not adjusted for seasonal compensation patterns.

Note: IEI, Section 2.1 clearly provides that price proposals submitted as responses in Phase I (for purposes of designating QLPs) operate as ceiling prices for work assigned in Phase II. At the time a specialized wholesale collection flow is assigned or bid in Phase II, QLPs must justify, in writing, any proposal to charge a price over and above the ceiling price, based on special processing requirements identified in an SOW, which are beyond the scope of the pricing template. As a general rule, FMS believes the pricing template for specialized lockbox addresses all anticipated requirements. Thus, FIs are advised that such requests to approve a change over the ceiling price for specialized wholesale services will only be granted by FMS in clear and convincing and exceptional cases. The ceiling prices applicable to retail and wholesale will not be waived.

3.4.5 Security Response

GLN security requirements are extensive and detailed commensurate with the importance of maintaining the integrity of Federal cash management operations. Respondents must certify that, if selected as a QLP, they will satisfy the mandatory technical requirements specified in IEI, Section 4.0, including, but not limited to, the security requirement detailed in IEI, Section 4.10 (physical and personnel security) and Section 4.11 (information technology), within 30 days of signing the DFA.

The Security Certification Statement must be submitted as the FI's security response to this IEI (see Attachment G on FMS' Web site: www.fms.treas.gov/rebids/attachments).

As noted above, the security response will be evaluated on a pass/fail basis. A failure to meet the security requirements of this IEI will result in automatic disqualification as a QLP, i.e. designation as a QLP is contingent on meeting the security requirements.

Note: Final security documents must be provided and requirements completed before a QLP can bid on or be assigned new business (see IEI, Section 4.10, Section 4.11, and Section 3.3 – Security Deliverables schedule). The security documents must include timeframes for physical and personnel security reviews by FMS at the proposed sites. FMS will approve the final security documents by the end of December 2003. The goal is to have the final QLP certification by FMS, authorizing the QLP to perform general lockbox services by ***January 2004***.

3.4.6 Innovations and Bonus Points

As stated above, FIs are encouraged, but not required, to submit proposed innovative ideas to improve the GLN. Approved innovations may result in the FI being awarded 1-10 bonus points which will be added to the FIs evaluated score. Ten points is the maximum aggregate bonus points that will be awarded by FMS to an FI, even if more than one innovation is approved and accepted. The bonus points awarded will be applied to each proposal (Region and subcategory of service) to which it pertains; therefore, the FI's proposal should make clear to which region and subcategory the innovation applies.

If the innovation(s) is approved by FMS, and the FI is designated as a QLP, the FI will pilot the innovation(s) in a particular region, for an identified subcategory: retail, wholesale, specialized wholesale.

By submitting a proposed innovation in response to this IEI, the FI acknowledges that FMS reserves the right to roll out the accepted innovation across the GLN where it would be implemented by other GLN QLPs to improve lockbox services provided to Federal agencies.

3.5 Designation of Qualified Lockbox Providers (QLP) Under the IEI

Process for Subsequent Assignment of Work to QLPs

Under this IEI, FMS is soliciting proposals from FIs interested in being designated by FMS as GLN QLPs for retail, wholesale, and specialized wholesale lockbox services in one or more of the following five distinct geographic Regions that comprise the reconfigured GLN:

Region 1 – North East
Connecticut, Delaware, Maine, Maryland, Massachusetts, New Hampshire, New Jersey, New York, Pennsylvania, Rhode Island, Vermont, Washington, DC

Region 2 – Mid-West
Illinois, Indiana, Iowa, Kentucky, Michigan, Minnesota, Missouri, Ohio, Tennessee, Wisconsin

Region 3 – South East
Alabama, Arkansas, Florida, Georgia, Louisiana, Mississippi, North Carolina, South Carolina, Virginia, West Virginia

Region 4 - Central
Colorado, Kansas, Montana, Nebraska, New Mexico, North Dakota, Oklahoma, South Dakota, Texas, Wyoming

Region 5 – West Coast
Alaska, Arizona, California, Hawaii, Idaho, Nevada, Oregon, Utah, Washington

A map reflecting the states assigned to the five Regions is listed in section 3.6.[2] FMS anticipates designating one or more QLPs in each Region in each lockbox sub-category: retail, wholesale, and specialized wholesale lockbox, at the conclusion of the IEI competition. Across the GLN as a whole, FMS estimates that approximately seven to ten different FIs will be designated as QLPs.

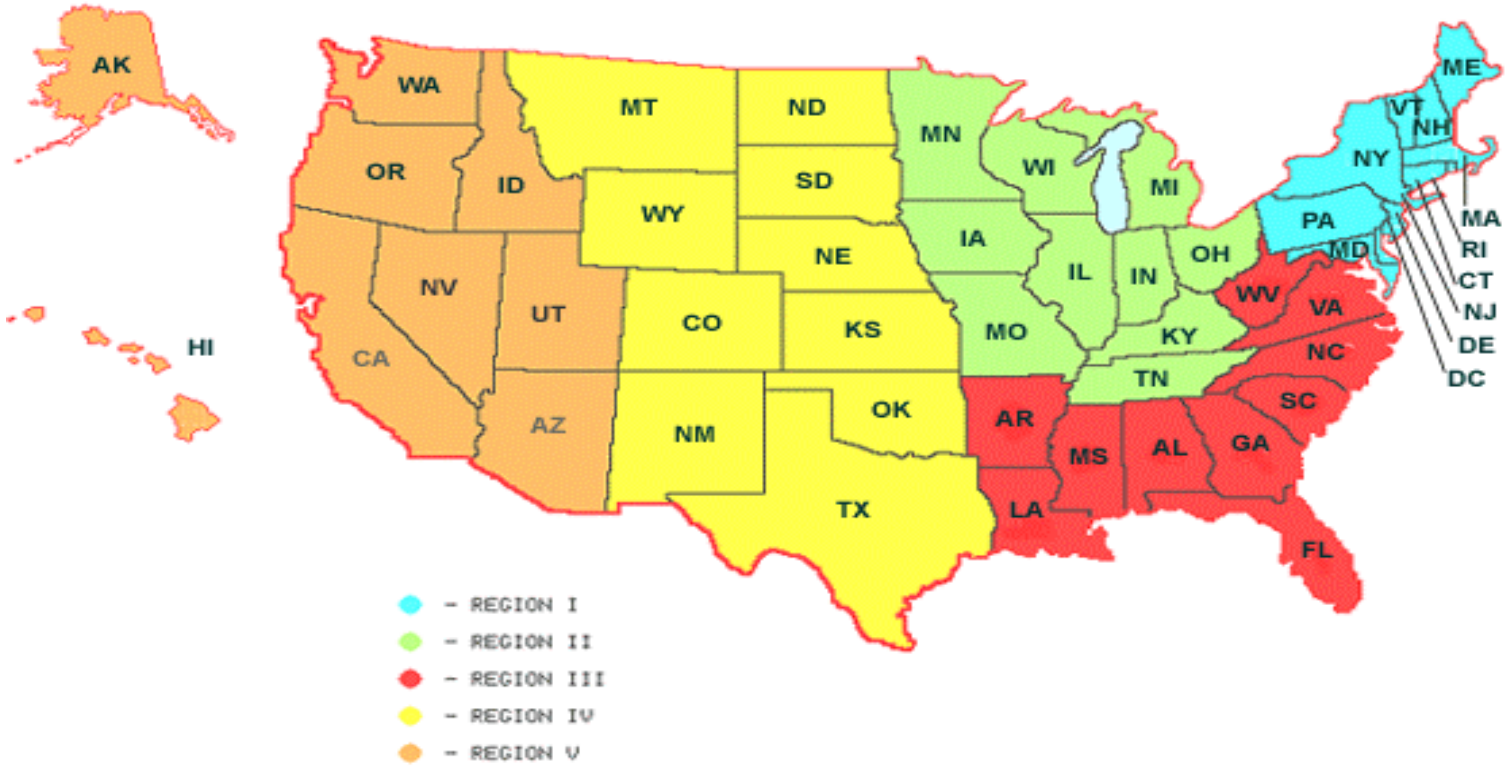
[2] FMS reserves the right to modify the configuration of the GLN Regions and/or the states assigned to the GLN Regions at any time during the IEI competition, or during the term of the GLN, upon a determination that it is in the best interests of the United States to do so.

Here is an example of a designation pattern that may result from Phase I. The examples below are aligned with the selection process examples shown in IEI section 2.1.

	Retail	Wholesale	Specialized Wholesale
Region 1	QLP A QLP B QLP C	QLP A QLP B QLP C	QLP A QLP B
Region 2	QLP D QLP E QLP F	QLP D QLP E	QLP D QLP E
Region 3	QLP A QLP E	QLP A QLP E	QLP A
Region 4	QLP C QLP F	QLP D	QLP D
Region 5	QLP E QLP F QLP G	QLP E QLP F QLP G	QLP E QLP F QLP G

This pattern is provided for illustrative purposes only. The actual QLP designation pattern/array will be determined by FMS upon the review and evaluation of submitted responses.

3.6 General Lockbox Network Processing Regions – Map



4.0 TECHNICAL REQUIREMENTS

4.1 Technical Requirements - Introduction

This section of the IEI contains general lockbox processing requirements for QLPs participating in the Treasury's GLN. These requirements address standard Federal agency collection needs but should not be considered inclusive of all Federal agency requirements. Specific processing requirements for individual lockbox accounts will be defined during the implementation phase for each account and specified in an account-specific Statement of Work (SOW), which will be attached to a memorandum of understanding (MOU) entered into by and among the QLP, FMS, and the Federal agency requiring lockbox services.

The general processing requirements, in this IEI, are grouped into three categories: retail, wholesale, and specialized wholesale lockbox processing. Processes common to all three categories are presented once as "Core Processing Requirements for All Categories" (see Section 4.4.1). Additional requirements distinguishing the categories follow separately.

4.2 General Requirements

QLPs shall be required to provide the services necessary for the preparation and planning for lockbox transitions (where necessary) and implementations. The characteristics of each collection stream vary in volume, timing, and origination.

In general, preparatory activities to begin lockbox collections begin with reviewing current agency receipts and processing practices. This review may require on-site visits to Federal agencies and/or presentations of paper lockbox fundamental processing and procedures.

In tandem with FMS, the designated QLP will assist agencies with defining specific requirements for the individual collection streams. The individual details of each process will be captured in an SOW.

4.3 Performance Measures

A QLP will be held to the highest standards of performance and quality. At a minimum, a quarterly review of work in progress and daily output must be performed by the QLP, the results of which are reported to FMS and the Federal agency involved. Additionally, the QLP must perform ongoing daily quality control review of work in process and daily mailouts. FMS will review the established quality controls to ensure that performance meets established standards. This review will include ensuring that quality measurements are defined by the QLP, measured and reported regularly, and monitored for performance within the standards set by the agency and FMS. FMS monitoring processes will also include periodic on-site reviews. Prior to the

commencement of lockbox processing under the new agreement, FMS will provide the selected QLPs with the performance measures that will be required for quarterly reporting.

Each quarter, the QLP shall submit in writing: (1) information on the QLP's overall goals or standards for each specific measure, and (2) the QLP's actual performance in meeting these measures for its government customers' lockboxes. The QLP may also provide any additional measures that it feels would be important. FMS recognizes that quality performance standards may change depending on the specific requirements for a particular lockbox application. At a minimum, quality measurement standards will display performance as it relates to:

Accuracy – the ability to provide service according to established procedures and instructions without errors.

Work Volume Accountability – the ability to establish control over work volumes as early as possible.

Workload Tracking – the ability to locate items at any point in the workflow process.

Responsiveness – the ability to respond to customer inquiries and problems so that customer expectations are met.

Timeliness – the ability to provide services within established deadlines or turnaround times.

System availability – the ability to make information and services available to customers within agreed upon timeframes.

Security – the ability to meet personnel, physical and information security requirements.

4.4 Processing Requirements

4.4.1 Core Processing Requirements for All Categories

The following procedures represent a description of the general services necessary to support standard processing for all categories of agency work in the general lockbox environment. The selected QLPs shall perform the services below as required by the SOW:

Mail Collection

Collect mail from the post office in accordance with the negotiated agency mail pickup requirements. FMS and the Federal agency must be notified in writing prior to any changes in this schedule. Mail pickup schedules should be established to collect 90% of the day's mail in time to complete same-day processing.

Use a unique ZIP code or some other means to expedite mail delivery and to distinguish collection streams (or accounts).

Use a separate identifier such as a post office box number or department number for each agency collection stream. This separate identifier must ensure a distinction between each collection stream in accordance with agency and FMS requirements.

Pick up all mail on the first pass at the destination Area Distribution Center (ADC) or Sectional Center Facility (SCF) in each location.

Receive express mail or other special deliveries at the lockbox site and process according to the SOW. Certified and registered mail shall follow SOW guidelines.

Establish controls as items are received.

Mail Processing

General lockbox extraction processes shall not be co-mingled with non-government extraction processes in the same space. Government incoming mail shall be segregated from corporate mail and other non-government media prior to extraction (see Security Requirements in Section 4.10, Technical Requirements). The following are detailed requirements for processing mail received by a QLP.

1. Process all mail received for each agency collection stream to insure same-day ledger credit in accordance with QLP processing schedules.

2. Process all mail on a first-in/first-out basis.

3. Begin each daily processing cycle at a designated time.

4. Notify FMS and the appropriate agency immediately if items received in a business day are not processed within the designated business day cycle and in accordance with the QLP's operating schedule.

5. Open the envelopes and extract the contents. Use automated extraction equipment wherever possible. Provide efficient alternative means for opening non-standard mail, fats, and flats.

6. Review the contents of the envelope to determine whether remittances are processable or unprocessable according to specific instructions in the individual agency SOW.

7. Candling of envelopes may be requested by an agency and shall be performed during extraction at the opening station. A second candling shall be performed daily upon request from the agency.

a. Checks and correspondence that are discovered in the candling process which cannot be re-associated with the original mailing shall be identified as "found in candling" and sent to the agency within one day of discovery.

b. A daily-itemized log of checks and documents found in final candling shall be maintained for one year. Each item found shall be entered into the log, using all available information. Information shall be entered regardless of whether the found checks/documents can be re-associated with the original mailing information. A copy of this log shall be sent to the agency on a monthly basis. The QLP shall perform periodic reviews of the final candled envelopes.

8. Date-stamp all unprocessable items and correspondence upon receipt, assemble per agency instructions, and forward to the agency within one business day. Establish a count control of all unprocessable items and correspondence. Establish a dollar value for auditing purposes, agency by agency where possible or as stated in the SOW.

9. Follow procedures in the SOW for handling the contents of remittance envelopes that do not contain a check or valid credit or debit card authorization, follow procedures in the SOW for handling the contents. At a minimum, this will include marking the envelope with a "C" (for cash) and an ID Number and forwarding the items to the agency.

10. Forward correspondence to Federal agency as specified in SOW.

11. Examine the enclosed remittances for negotiability and acceptability. Acceptable forms of payment include:

a. Personal checks
b. Corporate checks
c. Money orders
d. Certified checks
e. Cashiers' checks
f. Cash
g. Credit or debit card payment authorizations as allowed by the SOW
h. Treasury checks (FMS discourages Federal agencies from paying each other with Treasury checks. This practice, however, continues to exist and QLPs may receive Treasury checks in certain lockboxes. QLPs may need to forward Treasury checks (along with a SF 215 Deposit Ticket) to the closest Federal Reserve Bank (FRB), which will serve as the bank of first deposit. Documentation originally accompanying the Treasury checks will be processed according to the SOW.)

Coupons, gift certificates, and gift cards are considered as non-negotiable instruments for lockbox processing, and, therefore, should be forwarded to the agency for handling.

12. Process credit or debit card payment authorization allowed by the SOW, process in accordance with the Plastic Card Network (PCN) instructions in Section 4.5.

13. Examine check and money order remittances for the following conditions:

a. Acceptable payee as specified in the SOW.
b. Check dates:

i. Stale Dated – if the date is six months or more prior to the receipt date, the remittance shall be considered stale dated and forwarded to the agency,

ii. Post Dated – if the date is more than three days beyond the receipt date, do not process the payment. Forward it to the agency for disposition,

iii. No Date – write current date and process,

iv. Timeliness – Agencies may require stamping the remittance document or entering a date received, as specified in the SOW.

c. Differing amounts – Compare the legal and courtesy amounts on the check with each other and with the amount paid on the remittance document. If one of the three amounts differs from the other two, process according to the two amounts that match. If all three amounts differ, process according to the legal amount on the check (according to an individual SOW, a QLP may reject any checks with differing amounts for consumer checks).

d. Missing signature – Affix an "Arrange to Be Honored" sticker (or a stamp impression requesting the drawer FI to contact drawer for authority to pay) and process (according to an individual SOW, a QLP may reject any checks with missing signatures for consumer checks).

e. Foreign checks

i. Foreign checks drawn in U.S. dollars and payable through a U.S. financial institution shall be processed,

ii. Foreign checks payable in U.S. dollars drawn on foreign banks, or payable in foreign currency drawn on foreign banks shall be forwarded to the agency for disposition, along with all associated documentation.

a) Restrictive endorsements – process according to the SOW.

b) Checks endorsed "Paid in Full" – process according to the SOW.

c) Third party checks - if a check is endorsed over to the Federal agency or any acceptable payee specified by the Federal agency, or simply

endorsed and accompanied with an agency document, then deposit check as a regular payment.

(Note: Instructions relevant to this paragraph may vary by collection streams.)

14. Account for incoming and outgoing items – make sure that volume of incoming mail equals the deposited item count plus the number of unprocessed items.

Remittance Processing - General

1. Process remittances adhering to minimum service requirements and each agency's requirements as specified in the individually negotiated SOW. Minimum service requirements include sorting the documents into the following batch categories:

a. Single remittance with a single remittance document and the amounts match.

b. Single remittance with a single remittance document but the amounts do not match.

c. Single remittance with multiple remittance documents.

d. Single remittance document with multiple remittances.

e. Remittances without a remittance document. Process and key-enter the data and attach a photocopy of the remittance to the envelope. Where possible, all data capture information is key verified.

2. Separate checks and documents into batches and send to a multipurpose workstation.

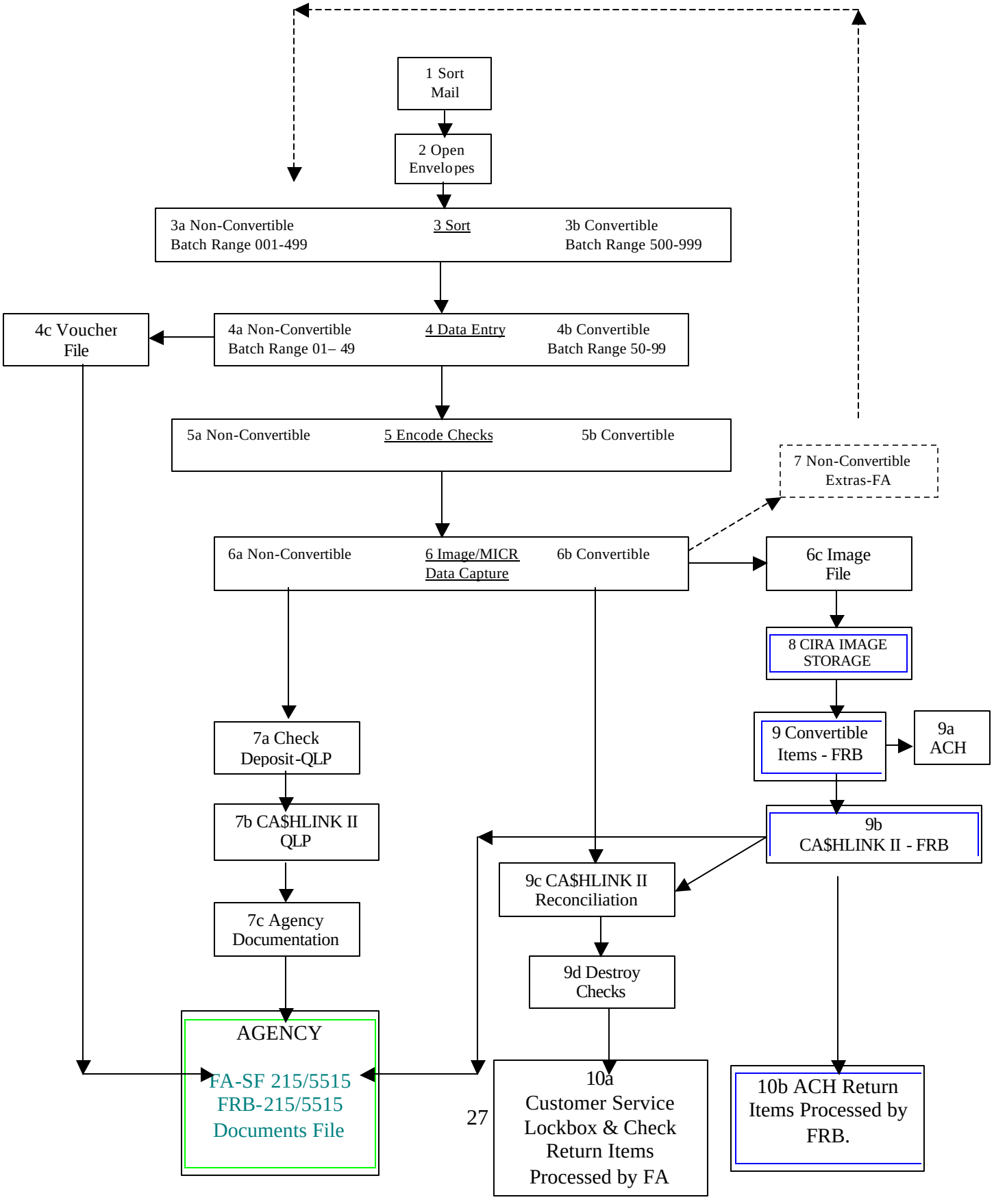
4.4.1a Check Processing

Over a period of time, FMS will be working with the QLPs to implement FMS' Paper Check Conversion (PCC) Program in the lockbox accounts. PCC is known in private industry as "eCheck" or "Accounts Receivable Conversion (ARC)" and converts paper checks received through the mail or drop box into electronic ACH debits to the check writer's account. Processing within FMS' PCC Program is significantly different from check processing or check conversion for a typical commercial lockbox account. For example, checks converted to ACH debit entries at a lockbox maintained for Treasury, are governed by 31 CFR Part 210, and applicable National Automated Clearing House Association rules, rather than the Uniform Commercial Code. Any given lockbox account may have checks that are convertible to ACH and checks that are not convertible to ACH. For those checks that are convertible, the QLP will be expected to use the **Paper Check Processing (PCC) (convertible items)** described in Part 1 below. For those checks that are non-convertible, the QLP will be expected to use the **Typical Check Processing** described in Part 2 below.

Note: FMS or the Federal agency will be responsible for fulfilling notification requirements to remitters for lockbox accounts where PCC is employed.

FMS and the QLPs will manage the transition from accounts that function with typical check processing to those that will function with Paper Check Conversion. Until these transitions occur, QLPs will use the procedures outlined under **Typical Check Processing**. The following Check Processing Workflow Diagram depicts the processing flow for convertible and non-convertible items. Each separate process is identified by a number or number/letter combination on the diagram that is used in the following process descriptions.

Check Processing Workflow Diagram



1. Paper Check Conversion (PCC) Processing (convertible items)

The PCC process is a highly automated multi-redundant system that greatly improves the collection, reconciliation, research and reporting processes associated with Federal agency check collections.

All images of the PCC items are retained in the Central Image and Research Archive (CIRA) for seven years or longer if the agency has a need to store the images for a longer period. The CIRA is maintained within the Treasury Web Application Infrastructure (TWAI) environment operated by the Federal Reserve Banks (FRB).

Remittance Document Imaging is a digital electronic representation of a remittance document, which may also be stored in the CIRA. This process eliminates forwarding paper copies of remittance documents to the agencies, which facilitates retrieval of document and payment information much faster. QLPs will continue to send data files to agencies or the Central Reporting System on a daily basis where applicable.

The CIRA is an on-line central repository for all PCC check images, associated financial information and other agency data that may be captured at the time of the transaction. It is a password-protected Web site, and login IDs are assigned by the FRB-Cleveland. From the time the transactions are uploaded in batch form during published processing hours to the CIRA, they are available for viewing within minutes. Agencies or QLPs will be able to access PCC data through the CIRA, and will have the ability to generate reports. The CIRA facilitates in researching an item or pulling down reports in multiple file formats.

The QLP shall be responsible for converting checks from paper to ACH transactions as directed in writing from FMS and/or the SOW at or below the ceiling price contained in the QLP's Pricing Response.

The QLP shall perform Paper Check Conversion (PCC) lockbox services in accordance with 31 CFR Part 210, as may be amended from time to time, and the "United States Treasury Financial Management Service Paper Check Conversion Standard Operating Procedures (PCC SOP)," dated May 30, 2003, as may be amended from time to time. (See IEI Attachment C on FMS' Web site www.fms.treas.gov/rebids/attachments.) FMS may revise these procedures from time to time with at least 60 days advance written notice to the QLP for a material change and 7 days notice for a non-material change or earlier if upon the mutual agreement of the parties.[3]

Low Volume/High Volume PCC Throughput

A QLP may use its own equipment when processing low- or high-volume PCC cash flows, as long as the PCC transactions are formatted according to the PCC specifications. QLPs may use Treasury's off-the-shelf PCC system for low volume lockbox operations, but are encouraged to adopt their own systems to the requirements of PCC.[4]

[3] Capitalized terms and acronyms not defined herein have the meaning set forth in the SOP.
[4] Each PCC system can process up to 2,000 items a day depending on the complexity.

Low Volume Processing Steps

1. Sort mail (1)

Mail is received at the lockbox processing facility and sorted in lockbox number order. In select cases, a Post Office (PO) Box is used and no sorting is necessary.

2. Open Envelopes (2)

Mail is distributed to the processing desk(s) where the following occurs:

a. Contents of the envelope are removed and reviewed for check negotiability.
b. Check amounts are compared to the voucher amounts.

3. Sort – Convertible and Non-Convertible Items

a. The QLP shall use its best efforts in accordance with developed procedures to recognize and manually sort non-convertible items. FMS recognizes that the QLP may not detect all non-convertible items:
(3b) convertible items.

4. Data Entry (if applicable to the agency cash flow)

a. Any agency specific data from remittance documents should be captured using the existing capture method for all remittances: (batch ranges may be input separately).
(4b) convertible items

b. The detail information is used to create:
(4c) a Voucher file that is forwarded/transmitted to the Agency.

The voucher file will provide subtotals facilitating Governmentwide accounting (GWA) reporting. The nature of these subtotals will be specific to each agency application, and the details will be provided in the SOW for each application. In some cases, the subtotals will be based on a combination of GWA Information. In other cases, the subtotals will be based on key elements within the data associated with a collection transaction. These key elements are known as Classification Keys. The method for determining the subtotals and the data elements involved will be outlined by the agency in the SOW. The subtotals will be part of the CA$HLINK II document prepared by the PCC Fiscal Agent and the sum of the subtotal amounts on each document must equal the total document amount. Accordingly, the QLP must provide the subtotal information to the PCC Fiscal Agent in such a way that it can be associated with the proper CA$HLINK II document.

5. Encode Checks (5b) (if applicable)

a. Online entry reconciles checks against Step 4's Data Entry detail. (This step only

applies if data transmission.)

b. There are detailed instructions for adjusting incorrect cashier/operator entries. (See PCC-SOP Attachment C)

6. Image/MICR Data Capture (Convertible Items)

   a. The convertible items (6b) are scanned through the PCC system and the transaction record is created.

   b. The QLP's operator/processor will manually key into the system the dollar amount for convertible items, and any other agency specific data in the configurable fields provided in the PCC software.

   c. A transaction record includes system generated transaction date and time, Item Reference Number (IRN), dollar amount, and any other associated agency data that is manually entered by the operator.

   d. Additional agency specific data may be entered into PCC transaction record for future Central Image and Research Archive (CIRA) research by the agency, e.g., account number. The required data elements need to be defined and will vary by agency; however, the PCC process will not change.

   e. Depending on the remittance document and agency needs, the remittance document may be imaged and stored in the CIRA. The remittance document must be approved by FMS, if applicable.

   f. The file is balanced and reviewed before transmitting.

   g. The image and remittance information is used to create:
      The PCC Image File (6c), which is forwarded to CIRA.

   h. CIRA houses the images for agency and QLP viewing.

   i. The PCC total will be reconciled against the check amount total.

7. QLPs may use their own equipment and procedures to complete the above steps. However, the QLP must:

   a. Transmit the images and data to the TWAI in the specified PCC format.

   b. Use an FMS approved transmission tool, such as Connect: Direct with Secure Plan Option.

c. Use a transmission medium capable of handling the volume in a reasonable time. A reasonable time generally means no more than two hours after balancing. Higher volume cash flows may balance and transmit several times throughout the day if necessary.

8. Convertible Items (9) - FRB

a. FRB creates and originates the ACH debits for the converted items.

For returns (10):

1) If the returned item is an administrative return, i.e. the Drawee account has an ACH debit block, the FRB will create a paper draft and re-clear.
2) If the return item requires some type of Drawee account and/or routing number changes, the FRB will make these required changes and resubmit.
3) If the return is a NSF return, the FRB will follow the existing return item instructions to either resubmit or retire.
4) If a final return or the item is deemed uncollectable, the FRB will make an SF 5515 CA$HLINK II entry and notify the agency and QLP, if applicable.

b. CA$HLINK II (9b) - FRB

The FRB creates the SF 215s, creates the Deposit Ticket number and enters the ACH deposit total into CA$HLINK II.

1) The FRB e-mails or makes available online SF 215s/5515s to the agency. Copies of the SF 215s are e-mailed to the QLP to be kept with the associated converted items.

c. CA$HLINK II (9c) Reconciliation

1) The QLP reconciles the FRB's SF 215 with the converted total on Day 2 and reports any discrepancy to FMS. (See PCC SOP Adjusting Incorrect Entries, in the IEI Attachment C on FMS' Web site www.fms.treas.gov/rebids/attachments).

d. Destruction of Checks (9d)

(1) Within 14 calendar days of review of completed SF 215, the QLP destroys the original converted items but keeps a copy of the SF 215 for its record.
(2) The CIRA will keep an image of the check and the associated transaction data for a minimum of 7 years.

9. Returns & Customer Service

a. The FRB will provide customer service for PCC items. The QLP's customer service should be reduced overall, because the Federal agency will do more of its own customer service with the FRB. Likewise, any PCC related inquiries should be

referred to the FRB Customer Support Line. (See PCC-SOP)

b. The QLP follows the return item procedures as directed by FRB and set forth in 8a above.

Note: Additional PCC specifications or requirements will be provided to the FIs at a later date.

2. Typical Check Processing (Non–Convertible items only)

1. Sort mail (1)

Mail is received at the lockbox processing facility and sorted in lockbox number order. In select cases, a Post Office (PO) Box is used and no sorting is necessary.

2. Open Envelopes (2)

Mail is distributed to the processing desk(s) where the following occurs:

a. Contents of the envelope are removed and reviewed for check negotiability.
b. Check amounts are compared to the voucher amounts.

3. Sort – Convertible and Non-Convertible Items

a. The QLP shall use its best efforts in accordance with developed procedures to recognize and manually sort non-convertible items. FMS recognizes that the QLP may not detect all non-convertible items:
(3a) non-convertible

b. Non-convertible items include: third-party checks; demand drafts and third-party drafts that do not contain the signature of the receiver; credit card checks; obligations of a financial institution (e.g., travelers checks, cashier's checks, official checks, money orders, etc.); checks drawn on the Treasury of the United States, an FRB, or a Federal Home Loan Bank; checks drawn on a state or local government; and checks payable in a medium other than United States currency. (See PCC SOP in the IEI Attachment C on FMS' Web site www.fms.treas.gov/rebidsattachments).[5]

The QLP shall not attempt to convert items if, through its sorting process, it becomes aware that the items are not convertible under the Federal Government's Rules for Participation in the Automated Clearing House.

c. Non-convertible items may change over time as the law, regulations or FMS policies direct.

[5] The need to manually sort items may be eliminated by evolving technology, consistent with governing law. When the need to manually sort items is substantially reduced or eliminated, FMS expects to receive the benefit of downward price adjustments.

4. Data Entry (if applicable to the agency cash flow)

a. Any agency specific data from remittance documents should be captured using the existing capture method for all remittances: (batch ranges may be input separately).
(4a) non-convertible items.

b. The detail information is used to create:
(4c) a Voucher file that is forwarded/transmitted to the Agency.

The voucher file will provide subtotals facilitating Governmentwide accounting (GWA) reporting. The nature of these subtotals will be specific to each agency application, and the details will be provided in the SOW for each application. In some cases, the subtotals will be based on a combination of GWA Information. In other cases, the subtotals will be based on key elements within the data associated with a collection transaction. These key elements are known as Classification Keys. The method for determining the subtotals and the data elements involved will be outlined by the agency in the SOW. The subtotals will be part of the CA$HLINK II document and the sum of the subtotal amounts on each document must equal the total document amount. This information will be required for credits and debits to each lockbox account.

5. Encode Checks (5a) (if applicable)

a. All non-converted checks are encoded with the dollar amount.

b. Spray checks with an accurate and legible audit trail on the back, including date processed, transaction number, and amount received.

c. Endorse all checks received with the following minimum Treasury requirements:

i. Routing Transit Number of Processing QLP (ABA)

ii. Credit to Agency

d. Perform balancing as specified in the SOW.

6. Image/MICR/Data Capture (6a)

a. Capture an electronic image of the front and back of all checks processed. Images shall be in the formats specified by FMS in the SOW and available to the agency and/or FMS via the Internet, CD-ROM, e-mail, fax, or file transmission as specified in the SOW. Each check image shall have an Item Reference Number (IRN) associated with it. If the check was accompanied by remittance documents, the IRN associated with the check images shall match the IRN associated with the document images.

b. Retain check images for non-PCC items for a period of six and one-half (6 1/2) years. Upon written or oral request, the QLP shall provide to the agency, within two business days, a printed image or electronic copy of any check the QLP processed. If the timeframe cannot be met, an interim response explaining reasons for the delay shall be sent to the agency.

NOTE: QLPs may be required to retain check copies and/or images for an indefinite time, as directed by FMS, due to litigation court-mandated retention requirements (see Section 4.9.5).

c. While electronic image transfers to the agency are the preferred solution, in some cases the agency may require a photocopy of each check when it is processed. The photocopy will be in addition to the electronic image and routinely forwarded to the agency as specified in the SOW.

7. Specific requirements for deposit reporting through CASHLINK II and mail out of agency documentation for non-convertible items are provided in the next two sections (7).

8. Process cash received - If cash is received for any processable item, convert the cash to a QLP cashiers check, money order, or internal QLP document payable to the agency involved. If the item is unprocessable, convert cash of $1.00 or more to a QLP cashiers check or money order and return to the agency. If unprocessable and less than $1.00, insert cash into an envelope, marked as "C," staple to upper left corner of the document, and send to the agency. All cash received shall be listed in a log. A copy of the log shall be forwarded to the agency monthly. The log shall include all available information and an indication if the cash was processed or unprocessable.

4.4.1b Deposit Reporting/CA$HLINK II (Non-PCC Items Only)

The CA$HLINK II system is used to automate the movement of funds and accounting detail from FAs to the U.S. Treasury's General Account. Functions performed in the CA$HLINK II system by FAs include: accepting, compiling, and reporting agency deposits; transferring funds through the Automated Clearing House (ACH) network or by Fedwire; and preparing and reporting lockbox income and expense information on a monthly basis.

Deposit information collected by the QLP shall be reported electronically by entering data into a personal computer using Deposit Reporting software provided by FMS. The debits and credits that constitute **today's work** (day of deposit) are those received and processed before the cutoff time for same day credit and those items received or prepared before the cutoff for today's posting date (returned items or adjustments). The cutoff time for today's work shall be included in each presentation, but shall generally not be earlier than 2:00 p.m. local time.

The diagram below illustrates "today's work" for a 4:00 p.m. cutoff. Assume today is October 21 and this is a paper lockbox transaction.

Oct. 20	Oct. 21		Oct. 22	
4 p.m.	Midnight	4 p.m.	Midnight	4 p.m.
← For work in this time period →		← For work in this time period →		
"Today's Date" = Oct. 21		"Today's Date" = Oct. 22		
Date of Deposit = Oct. 21		Date of Deposit = Oct. 22		
Funds Transfer = Oct. 22		Funds Transfer = Oct. 23		

Below are the steps for deposit reporting for non-convertible items. Note the following procedure must be followed for all deposit reporting in CA$HLINK II, including deposit ticket, credit adjustments, and debit vouchers:

QLPs will be required to include, as part of each CA$HLINK II document, a breakout of the document amounts by one or more subtotals supporting Governmentwide accounting. The nature of these subtotals will be specific to each agency application, and the details will be provided in the SOW for each application. In some cases the subtotals will be based on a combination of Treasury Governmentwide accounting information. In other cases the subtotals will be based on key elements within the data associated with a collection transaction. These key elements are known as Classification Keys. The method for determining the subtotals and the data elements involved will be outlined by the agency in the SOW. The subtotals will be part of the CA$HLINK II document, and the sum of the subtotal amounts on each document must equal the total document amount. This information will be required for credits and debits to each lockbox account.

1. Checks forwarded for collection - Prepare a U.S. Treasury Deposit Ticket (SF 215) for the total amount of the daily tape or transmission file that is sent to the designated Agency Location Code (ALC) address. Only one Deposit Ticket per CA$HLINK II account number (a three-digit number representing each account in CA$HLINK II) is required; however, multiple Deposit Tickets may be used, if necessary. QLPs may generate their own automated SF 215 with the prior approval of FMS. If the SF 215 is typed and an error occurs, no corrections can be made to the document. The document shall be voided and a completely new Deposit Ticket prepared. Enter all appropriate SF 215 data into CA$HLINK II.

2. Returned checks - the following procedure shall be followed for any check that is not paid by the remitter's FI on which it was drawn:

a. Debit the demand deposit account for the total dollar amount of items not paid for any reason following second presentation or for those checks that cannot be recleared after the first presentation.

b. Prepare a U.S. Treasury Debit Voucher (SF 5515) daily for the total amount of the returned items and process accordingly. Enter all appropriate SF 5515 data into CA$HLINK II.

c. Forward returned checks to the agency with a prepared listing of the items (internal QLP debit memorandum), citing the date the returned items were posted to the account. Returned checks and debit memoranda shall be included in each day's accounting package.

3. Miscellaneous adjustments - Encoding errors or other deposit discrepancies (other than return items) shall be handled as follows:

a. For each debit adjustment to the account, a Debit Voucher (SF 5515) shall be completed detailing the nature of the adjustment. Enter the original deposit date from the Deposit Ticket (SF 215) in box 2 and current date in box 6. Enter all appropriate SF 5515 data into CA$HLINK II.

b. For each credit adjustment to the account, a Deposit Ticket (SF 215) shall be completed detailing the nature of the adjustment. Enter the original deposit date from the SF 215 in box 2 and current date in box 6. Enter all appropriate SF 215 data into CA$HLINK II.

c. Documentation explaining both debit and credit adjustments shall be attached to the Deposit Ticket or Debit Voucher.

d. Debit and credit adjustments documentation will depend on the type of adjustment. At a minimum, any adjustment documentation must include a copy of the check (front and back) for encoding errors. Any other documentation necessary to explain the adjustment (such as a copy of the deposit ticket correction) shall be included.

Note: FMS reserves the right to accelerate the transfer of deposits to occur on the day of deposit.

Mailout

Mail remittance, accounting documents, and/or tapes to the Federal agency in accordance with the instructions in the SOW. All documents and tapes shall be packaged securely. First-class and overnight mailout deadlines shall be established to meet agency-specific needs.

Data Transmission and Reports (Interim Process)

1. The QLP will transmit deposit detail transaction data electronically and securely in formats specified by FMS in consultation with the agency. Initially, as an interim solution, the QLP will be required to transmit such files directly to the agencies, with formats, connectivity requirements, and encryption specified in the SOW.

2. In some cases, a daily data tape exchange with the agency may be necessary until data transmission requirements have been defined and testing has been completed. The following procedures shall be followed:

a. The tape shall be sent to the agency with the daily mailout package. When the data transmission begins, the transmission shall occur during a mutually agreed upon-time, Monday through Friday. Weekend activity shall be included in Monday's transmission or next business day, except during peak periods (for specific agencies), when it shall be done every day.

b. System back-up tapes shall be maintained for thirty (30) calendar days, unless specific circumstances require an extension. Back-up and/or duplicate tapes shall not be shipped to the agency.

c. When a replacement tape is requested, it shall be recreated and shipped to the agency with the next shipment after notification. The replacement tape(s) shall be identified and labeled "Replacement Tape(s) for MMDDYY – Replaces Tape 1XXXX."

d. The QLP shall provide any updated program documentation necessary for testing annually, prior to Quality Systems Testing.

3. In some cases, computer printouts or CD ROMs of daily transactions will be mailed to the agency.

4.4.1c Data Transmission and Reports (Central Reporting System (CRS))

The Financial Management Service will be developing a Central Reporting System (CRS) that will enable Federal agencies to more effectively manage the financial transaction information resulting from FMS' collection processes. This effort will greatly improve the way government agencies collect, analyze, and redistribute financial transaction information. In addition, the CRS will eliminate redundancies and disconnects across and between the numerous point-to-point connections currently in place between collection points and Federal agencies. After the implementation of the CRS system, each QLP will be required to transition the distribution of this information from the individual Federal agencies to a single touch point within the CRS. QLPs must have Burstable T-1 or T-3 lines available for transmission to FMS. Data transmissions will be required to comply with standard government-wide XML schemas. As mentioned above, the CRS platform will be established as an open architecture based on the XML standard. As a centralized system, the CRS will offer a suite of electronic information services that Federal agencies can use to meet their financial management and reporting responsibilities. Specifically, the CRS will, at a minimum, provide for the following:

Consolidated Financial Transaction Reporting: The CRS will collect, normalize, and retain detailed financial transaction information from all collection systems in use by Federal agencies.

Single Touch Point: The CRS will provide Federal agencies, QLPs, and Federal Reserve Banks with a single touch point for the exchange of all financial transaction information across all collection systems.

Summary and Detailed Transaction Information: Provide standard and customized financial information reports to Federal agencies on a real-time basis.

Daily Collection Summaries: Provide Federal agencies with a single, consolidated, daily report of all revenue activity across all collection systems.

Real-Time Inquiries: Provide Federal agencies with the capability to review detailed and summary transaction information by Government-wide accounting (GWA) Information.

Data Distribution: Provide data transfers (downloads) in standard formats to enable agencies to further manipulate transaction information on in-house systems.

Standard Financial Information Exchange Formats: Establish and utilize standard government-wide XML schemas for all collection transactions.

The CRS system is scheduled to be implemented in 2004. Consequently, it will be necessary for each QLP to modify its collection systems to comply with FMS' standard data formats and single distribution point after the CRS is implemented. After implementation, the detailed transaction information will be sent to FMS via the CRS rather than each individual agency. Once reporting requirements have been changed and QLP processes streamlined, FMS will ask for price adjustments to reflect these efficiencies.

4.4.1d Internet Check Matching via Pay.gov

The QLP shall be required to fulfill "Internet matching" services if required by a Federal agency. Internet matching is the process of matching a paper check received at a lockbox location with associated remittance information, such as completed forms, that have been submitted online at the Pay.gov Web site. Pay.gov is a Government-wide transaction portal managed by FMS that offers a suite of electronic financial services to assist Federal program agencies. See Pay.gov information on FMS' Web site at www.pay.gov.

With some cash flows, Federal agencies require the option of allowing a remitter to file detailed information about a transaction or set of transactions online, including the upload of large files of program information, but with the associated payment delivered by check to a lockbox. In these cases, Pay.gov will host the online filings, and the QLP will operate the associated lockbox. The QLP shall be required to:

1. Receive the paper checks and process them through the lockbox.
2. Receive a file from Pay.gov of transactions conducted online.
3. Match the Pay.gov filings and lockbox receipts based on transaction identifiers assigned by Pay.gov.
4. Send files to Pay.gov or the agency showing matched and unmatched items.

File formats shall be specified by FMS.

4.4.1e Customer Service

The QLP shall designate a customer service liaison (name, telephone, etc.) to receive all Federal agency customer service requests. The QLP customer service liaison or his/her representative shall receive and log all written requests to research processing errors, excluding photocopy requests, and shall provide a written response within five (5) business days or as specified in the SOW (fewer days may be desired). Where extensive research is required, an interim written response will be sent to the requestor. Special expedited processing shall be required on Congressional, Judicial, and "priority" requests, in any case no more than 2 business days. Agencies should provide all pertinent information to the QLP when requesting customer service assistance regarding processing errors including: deposit date, batch/block number, batch/block dollar total, sequence number, and the dollar amount. All QLP customer service unit responses shall include, as a reference, a copy of the Federal agency's initial written request for assistance. The QLP customer service unit shall respond to all inquiries within one (1) business day. Telephone logs should be developed and maintained to indicate name of Federal agency; processing error(s) including deposit date, batch number, batch dollar total, sequence number, and the dollar amount; and Federal agency contact information including telephone number. The QLP will prepare a written interim response to Federal agencies when significant delays are encountered or anticipated.

The QLP will prepare quarterly customer service reports to FMS. The QLP shall cooperate fully in remedying customer service issues identified by FMS and the agencies.

4.4.2 Processing Requirements – Retail Lockbox

Generally, a retail lockbox will have a scannable document returned with the remittance. A scannable document is one that possesses the line of machine-readable information that a Federal agency prints on payment documents or documents. The following procedures represent a description of the general services necessary to support standard agency **retail** lockbox processing. The QLPs shall perform the services below as required by the SOW:

Core Processing Requirements

Retail lockbox processing requirements include the core processing requirements identified above as well as the additional services specific to retail accounts.

REQUIREMENTS SPECIFIC TO RETAIL LOCKBOXES

1. Process remittance documents through an automated processing system to capture data encoded on the scan line of the remittance document. The scan line shall be captured and stored electronically for reporting to the agency.

2. For remittance documents with no scan line, or if the scan line is unreadable, key-enter the appropriate fields from the remittance document as outlined in the SOW. All key entered data are to be key-verified.

3. Disposal of envelopes/coupon – Forward to the agency or destroy, as specified in the SOW. Add imaging of envelopes/coupons to perform timeliness inspections.

4. Change of address - If the change of address box on the remittance slip is marked, the remittance slip will be returned to the agency after regular payment processing. The QLP shall have the capability to create a file of address changes if required by the agency.

4.4.3 Processing Requirements – Wholesale Lockbox

Generally, a wholesale lockbox will not have a scannable document returned with the remittance. Instead, there will be one or more documents relating to the remittance that may require some form of data capture. However, all wholesale lockbox providers under this SOW must be prepared to accept and process scannable documents in addition to other remittance documents as the need arises.

The following procedures represent a description of the general services necessary to support standard agency **wholesale** lockbox processing. The selected QLPs shall perform the services below as required by the SOW.

CORE PROCESSING REQUIREMENTS

Wholesale lockbox processing requirements include the core processing requirements identified above as well as the additional services specific to wholesale accounts.

REQUIREMENTS SPECIFIC TO WHOLESALE LOCKBOXES

1. If there is a scannable remittance document (coupon), process the remittance document through an automated processing system to capture data encoded on the scan line. The scan line shall be captured and stored electronically for reporting to the agency.

2. Change of address – If the change of address box on the remittance coupon is marked, return the coupon to the agency after regular payment processing. The QLP shall have the capability to create a file of address changes if required by the agency.

3. Flatten invoice and/or other remittance documents as specified in the SOW.

4. Sort remittance documents and perform other document handling tasks as specified in the SOW.

5. Process relevant remittance documents through an imaging or Intelligent Character Recognition (ICR) system to facilitate data capture of fields required by the agency. Correct and supplement captured fields via key entry or other technology (i.e., voice recognition). Captured data shall be stored electronically for forwarding to the agency.

6. Disposal of envelopes/remittance documents – Forward to the agency or destroy, as specified in the SOW. Add imaging of envelopes/coupons if specified in the SOW.

4.4.4 Processing Requirements – Specialized Wholesale Lockbox

Generally, a specialized wholesale lockbox will be similar to other wholesale lockboxes in that there is no scannable document returned with the remittance but rather it will have one or more documents relating to the remittance. What distinguishes this category is that the accompanying documents involve more complex business rules (e.g., validations) and document handling procedures, e.g., imaging both sides of the remittance document. In addition, security requirements (addressed in Section 4.10) may be higher in one or more of the areas of physical, personnel, document, and information security. Only FIs able and willing to perform highly manual and customized processing and meet higher security requirements should express interest in this category.

The following procedures represent a description of the general services necessary to support agency **specialized wholesale** lockbox processing. Because of the unique and involved requirements for each of these applications, the details of the processing requirements will vary greatly by application and will be fully defined in the SOW. At a minimum, however, the selected financial institution(s) can expect to perform the services below.

CORE PROCESSING REQUIREMENTS

Specialized wholesale lockbox processing requirements include the core processing requirements identified above as well as the additional services unique to each account.

BROAD REQUIREMENTS FOR SPECIALIZED WHOLESALE LOCKBOXES

1. Flatten invoice and/or other remittance documents as specified in the SOW.

2. Sort associated documentation and perform other complex document handling tasks and business rule validations as specified in the SOW.

3. Process relevant remittance documents through an imaging or Intelligent Character Recognition (ICR) system to facilitate data capture of fields required by the agency. Correct and supplement captured fields via key entry or other technology (i.e., voice recognition). Captured data shall be stored electronically for forwarding to the agency.

4. Destroy or forward all envelopes and remittance documents to the Federal agency as specified in the SOW. Often this task involves sorting documents for multiple daily mailouts.

5. Perform basic arithmetic computations for individual remittances or groups of remittances as specified in the SOW.

6. Conduct logical evaluations based on predefined criteria as specified in the SOW. For example, evaluate whether the appropriate fee has been enclosed for the type of application submitted or for other characteristics of the applicant such as age.

Examples of actual statements of work for specialized wholesale lockbox accounts are available upon request from prospective bidders.

4.5 Requirements for Credit Card/PCN Lockbox Processing

All credit/debit card transactions processed through the General Lockbox Network using the Federal Government's Plastic Card Network (PCN) must fulfill the following requirements.

CREDIT CARD PROCESSING FIELDS

The paper document that the lockbox processes must contain complete and legible:

1. Credit Card Number (16 digits)
2. Expiration Date of the card (4 digits)
3. Dollar amount
4. Card holder Billing Address
5. Open field for Agency Use
6. Open field for future card association required fields (additional Address Verification Services)
7. Field to capture security codes (additional 4 digits after credit card number)

If portions of the above requirements cannot be processed, the QLP must highlight the required field error and forward the document to the agency to research and remedy. An agency may specify additional requirements such as promotional codes.

4.5.1 Connectivity To A PCN Financial Agent

The lockbox must connect to a PCN financial agent for authorization. This can be either online, batch, or a combination of both. The detail as to how connectivity is accomplished, and on what platform, is dependent on the PCN financial agent.

Batch Authorization Information

The lockbox must be able to receive an authorization file back and post those collections to its other settlements for that day. Typically, the lockbox has one large collection file that contains cash, check, and credit cards aggregated together. Ideally, this requirement will be met through system integration; i.e., no manual file manipulation and no key entry.

DISTINCT PLASTIC CARD FILES AND TRANSACTIONS

When plastic card authorizations post as collections, the transactions shall be designated as credit or debit card and distinguished from cash, check, or other collections for accurate posting and reporting.

Adherence To PCN Rules

Participating agencies and QLPs must complete the appropriate applications, Agency Participation Agreements, and amendments in order to use the PCN to collect credit/debit cards.

4.5.2 Governmentwide Accounting (GWA)

The PCN financial agent is responsible for reporting into CA$HLINK II the collections and adjustments received via the PCN. If the QLP is not the same as the PCN financial agent, the QLP must forward to the PCN financial agent the data necessary to complete CA$HLINK II reporting, in particular subtotals facilitating Governmentwide accounting. The nature of these subtotals will be specific to each agency application, and the details will be provided in the SOW for each application. In some cases, the subtotals will be based on a combination of GWA information. In other cases, the subtotals will be based on key elements within the data associated with a collection transaction. These key elements are known as Classification Keys. The method for determining the subtotals and the data elements involved will be outlined by the agency in the SOW. The subtotals will be part of the CA$HLINK II document and the sum of the subtotal amounts on each document must equal the total document amount. Accordingly, the QLP must provide the subtotal information to the PCN financial agent in such a way that it can be associated with the proper CA$HLINK II document.

4.6 Check Processing Option – Check Truncation

In addition to paper check conversion process described in Section 4.4.1 (sometimes referred to as accounts receivable check (ARC) conversion), an alternative for clearing checks may include check truncation. Earlier this year, the U.S. House of Representatives passed H.R. 1474, Check Clearing for the 21st Century Act, also known as Check 21. It would allow FIs to truncate, or voluntarily exchange electronic images of checks instead of using paper checks, automating the clearing process. Currently, FIs are required to exchange the paper checks, which are subject to transport delays. Check 21 would also grant the same legal validity to images of checks as to the original checks themselves. Check truncation uses the same settlement process as paper checks; the payments are not converted into Automated Clearing House (ACH) transactions.

If the Check 21 Act becomes law, FMS will draft additional technical requirements as needed. FMS would then expect QLPs to truncate checks that are unable to be converted to ACH through the PCC process.

4.7 Imaging Enterprise Platform Concept

In this section, FMS provides notice that it is considering the development of a system platform (Imaging Enterprise Platform) to support lockbox-imaging services conducted at lockbox

processing sites of any QLP. This notice is a high-level concept paper and provides a preview of an intended offering. QLPs should acknowledge and understand that they shall be required to interface with and use the Imaging Enterprise Platform at the direction of FMS.

Purpose

FMS intends to offer imaging and automated decision-making technology to Federal program agencies:

1. To electronically capture information from agency forms and apply agency business rules,
2. Allow for the deposit of any associated fees through lockbox operations, and
3. Provide Federal program agencies the ability to track, balance, and monitor transactions through a Web Based processing platform through a unique identifier.

In addition, this technology will reduce costs by providing scalability, reducing redundant form-by-form development costs.

Concept

The Imaging Enterprise Platform will:

1. Accept from any QLP images and associated captured data, which data has been verified by the QLP prior to transmission. Images may include checks, forms, and supporting documents;
2. Apply business rules, established in conjunction with the Federal program agencies, to captured data;
3. Transmit to the QLP a file of accepted or rejected items;
4. Transmit all images, under specifications to be provided by Treasury, to the Treasury Web Architecture Infrastructure (TWAI) where the images will be stored and will be Web accessible to the QLP and the Federal program agency; and
5. Transmit daily file of processed items to Federal program agency, under specifications to be provided by the agency.

Detailed Statement of Work

A detailed statement of work will be included in the second phase of this rebid for any payment streams that will require use of the Imaging Enterprise Platform.

4.8 Contractors

Terms for Use of Contractors

A QLP may perform required lockbox processing services by utilizing other FIs or third parties only with the prior consent of FMS. Upon consent, the QLP shall provide to FMS, within 60 calendar days prior to implementation of general lockbox services for a Federal agency, a Contractor Plan, which, at a minimum, shall include:

Identification of the contractor's full name, complete street address, and phone number;

1. Evidence of the contractor's intent to participate;
2. The type of services to be secured through the contract and the percent of overall agency processing performed by the contractor;
3. The technical qualifications of the contractor;
4. A list of three professional references of the contractor that utilize the same services as will be provided to FMS;
5. A contingency plan to rectify any contractor work stoppage; and
6. The QLP's quality control plan for the contractor.

All contracts between the QLP and a contractor must be available for review by FMS upon request.

The DFA requires the QLP to perform depositary and financial agent services involving the collection and transfer of public funds to Treasury in accordance with the requirements of 31 CFR Part 202. Contractors who are not eligible and designated as depositaries and financial agents under Part 202 may not control or possess public funds at any time.

The proposed use of contractors shall be clearly explained in the FI's response to this IEI. A QLP remains solely responsible for the performance of its contractor(s). If used, contractors shall adhere to the same standards required of the QLP. Any change of contractor by a selected QLP requires prior written approval by FMS.

4.9 Audit and Report Requirements

4.9.1 Internal Audits

The QLP is required to conduct and prepare, at its own expense, semiannual internal audit reports of its lockbox operations. The QLP shall submit such audit report results to FMS within 30 calendar days of completion of the report. Audit reports shall be due no later than the last day of January and July of each year, unless alternative dates are mutually agreed upon by the parties in writing. FMS will evaluate these semiannual audit reports and track resolution of findings.

4.9.2 Independent Audits

The QLP is also required to obtain a biannual external audit (from an independent audit firm) of its lockbox operations using an SAS 70 Type II accounting or audit standard. The first report shall be due to FMS no later than one (1) year from the effective date of the first MOU/SOW entered into with any Federal agency pursuant to the DFA. Subsequent reports shall be due on the same date every two years, unless alternative dates are mutually agreed upon by the parties in writing.

4.9.3 Formal Dispute Process

General: FMS and the QLP agree that it is in their mutual interest to resolve disputes by agreement. If a dispute arises from the implementation or administration of this DFA, FMS and the QLP will make all reasonable efforts to resolve the dispute by mutual agreement.

Initiation of a Formal Dispute: If the dispute cannot be resolved informally by mutual agreement, the QLP and FMS will use the following dispute resolution mechanism:

> The QLP will submit to the Authorized Treasury Official (ATO) a written statement within 90 days of the aggrievement with supporting documentation in appendices that articulates the dispute, the QLP's position, the relief sought, and the methodology used to calculate or determine the relief sought. (The ATO is the FMS official authorized to act for and bind the U.S. Treasury regarding U.S. Government lockbox collections. Currently, the ATO is the Director of the Cash Management Directorate, Financial Management Service, U.S. Department of the Treasury.)
>
> The written statement will include a certified statement executed by an appropriate representative of the QLP (the Authorized Bank Official, or ABO), which states that:
>
> 1. The dispute or claim is presented in good faith;
> 2. Supporting documentation is accurate and complete; and
> 3. The amount of relief requested is accurate.
>
> The ATO will review the written statement and supporting documentation, and make a threshold determination on whether the dispute should proceed. Specifically, if the ATO decides that the dispute is without merit, the ATO will dismiss the dispute and so notify the QLP in writing. If the ATO determines that the dispute will proceed, the ATO will provide to any affected Federal agency the QLP's statement and supporting documentation.
>
> Within 30 calendar days of the date the ATO sends the QLP's statement to any other party, such other party may submit to the ATO a written response statement with supporting documentation in appendices. The responding parties are responsible for concurrently serving their responses to the QLP.

The ATO will issue a written decision within 30 calendar days after the period for submission of the response statements. The ATO may unilaterally extend this period for decision up to an additional 30 calendar days. The written decision of the ATO may order that specific actions be taken, including but not limited to:

1. Payment, method of payment, and payment due date(s) for Value of Funds Assessments,
2. Authorized fines,
3. Loss of Treasury Time Balance or Depositary Compensation Securities without recompense, and
4. Full or partial revocation of the DFA.

The ATO will send the written decision to all affected parties.

Payment: The amount determined payable under the ATO's decision, less any portion already paid, will be paid by the liable party in accordance with the ATO's decision.

Obligation to Continue Performance: The QLP shall proceed diligently with performance of the services required by the DFA pending final resolution of any claim.

Other Remedies: Notwithstanding the provisions of this section, the QLP, and FMS have the right to pursue any and all available legal or equitable rights they may have notwithstanding any written decision by the ATO.

4.9.4 Required Transition Services

The QLP recognizes that the services provided under this DFA are vital to the U.S. Government and must be continued without interruption, and that, upon the expiration or termination of the DFA, FMS may designate another QLP to provide the services required hereunder. Upon expiration of the DFA, the QLP shall, unless otherwise directed in writing by FMS, provide all approved transition services e.g., transporting remittances to successor and phase-in training of successor.

Compensation for Transition Services - The QLP will be compensated for all phase-in and phase-out transition services.

4.9.5 Document Retention/Schedules

A QLP (and its approved contractor(s)) performing general lockbox services for a Federal government agency shall maintain all books, records, reports, documents, and other evidence related to the performance of services, which will, among other things, properly support all claims for compensation, lockbox processing, and deposit activity. FMS reserves the right to examine, audit and obtain copies of any of the above without substantial delay and without charge. See the DFA, Appendix 1, for specific document retention requirements. Due to continuing litigation, the QLP must retain indefinitely (until further notice) all SF 215s,

SF 5515s, and any supporting documentation associated with transactions relating to deposits received from the following Federal agencies:

1. U.S. Department of Homeland Security/Bureau of Customs and Border Protection,
2. U.S. Department of the Treasury/Treasury Tax Bureau, and U.S. Department of Justice/Bureau of Alcohol, Tobacco, Firearms and Explosives
3. U.S. Department of the Interior and all bureaus and agencies of the Department of Interior.

As necessary, FMS may instruct the QLP that it must retain documents as required by any litigation involving FMS.

4.9.6 Account Analysis Formats

Minimum Lockbox Expense Reporting Requirements – QLPs will submit account analysis information to FMS on a monthly basis in both paper (preferably in Microsoft Excel) and the ANSI X.12 Account Analysis Transaction Set (822). The paper submission will include the following minimum reporting sections: Summary Account Analysis Statement, Account Summary, and Detailed Account Analysis Statement.

QLPs will prepare a Summary Account Analysis Statement and Account Summary for each processing site and will prepare Detailed Account Analysis Statements for each Demand Deposit Account (DDA). The Summary Account Analysis Statement and Account Summary will precede the Detailed Account Analysis Statements.

In addition, QLPs will provide FMS with Ancillary Charges Invoice Support and prepare a separate invoice for each Lockbox Account in Microsoft Excel format detailing the fiscal year ancillary expenses.

Examples of the above-mentioned lockbox expense reporting requirements can be accessed at FMS' Web site under the IEI Attachments section at www.fms.treas.gov/rebids/attachments.

1. **Summary Account Analysis Statement (Template) – Attachment D**
2. **Account Summary Information (Template) – Attachment E**
3. **Detailed Account Analysis Statement (Template) – Attachment F**

Ancillary Charges Invoice Support

QLPs in the GLN will provide FMS with invoices in Microsoft Excel format detailing ancillary expenses for each lockbox on an annual basis.

Invoice Due Date

Fiscal year (October through September) invoices are due to FMS by the last business day of October in each year of the Agreement.

Invoice Data Requirements

An invoice will contain the following administrative information:

1. Attention: Agency Contact Person, Agency, Telephone Number and E-Mail Address of Agency Contact

2. From: FMS Account Analyst Assigned to the QLP, FMS, and Telephone Number of Account Analyst

    a. Invoice-Fiscal Year 200X Ancillary Expenses
    b. Name of Agency
    c. Name of FI
    d. DDA Number
    e. Lockbox Number
    f. Agency Location Code

3. An invoice will contain the following ancillary services-related information:

    a. TMA Code
    b. TMA Description
    c. Unit Price for Each TMA Code/Description
    d. Monthly Volumes for each Service
    e. Monthly Expenses for each Service
    f. Total Fiscal Year Expenses for each Service
    g. Total Fiscal Year Ancillary Expenses

4.10 Security Requirements

The security requirements set forth in this section 4.10 are derived from FMS Security Manual, which was developed in furtherance of the Treasury policies contained in Treasury Directive 71-10.

4.10.1. Physical Security

Physical security of QLPs is required to ensure that adequate controls exist to detect and deter instances of theft, fraud, waste, and/or abuse of checks, remittances, negotiable instruments, and privacy act information. Physical security is the first line of defense as it pertains to attempted intrusion or internal theft, while acting as the last line of defense when all other counter measures or controls fail.

The security of QLP facilities requires the integration and implementation of intrusion detection systems (e.g., door alarms, motion detectors, etc.), closed circuit television (CCTV) monitoring, camera technology, video recording equipment, and other physical security controls.

QLPs are required to meet the security standards herein to protect government remittances and associated sensitive information, and mitigate the risk of the theft, loss, and compromise of sensitive but unclassified information.

The structure and location of the building combined with the scope and sensitivity of operations are the major considerations in determining appropriate security safeguards. The number of floors, doors, windows, fire exits, roof vents, along with the degree of ground-level access, and parking facilities all affect building security. The minimum-security standards for access controls for the perimeter of the building are as follows:

> Commercial, multi-tenant facilities must have security guards to perform access control duties, monitor personnel entering the facility (e.g., main lobbies, entrances designated for "employees only") and personnel reporting to loading dock/delivery areas. Security guards must be assigned to a security guard station or designated guard posts. The security guard station must be equipped with CCTV monitoring equipment (with the capability to observe and monitor entrances to the general lockbox processing area and other areas as required), duress alarms, land line telephone, internal communications (e.g., two-way radios), and post orders. Secondary guard posts should be equipped at an appropriate level that guards can perform effectively. Security guards must be required to physically touch each badge to verify the legitimacy of the badge and to match the badge photo with the face of the presenter, in the event card access controlled turnstiles, proximity cards, man-traps in conjunction with card readers, or other security controls/automated entry systems are not used to verify and validate personnel entering the facility.

If the facility does not have security guards to perform access control duties, then dedicated security guards assigned to the general lockbox processing floor are required. In cases where security guards are dedicated and assigned to the general lockbox processing floor, some form of access control for the building (e.g., main lobbies, "employee entrances," loading docks) is expected. The following are acceptable access control measures for entrances to facilities where general lockbox processing occurs and can be used individually or in combination:

1. Card access (e.g., photo identification, swipe, or proximity cards) controlled doors monitored by surveillance cameras combined with anti-piggybacking technology.

2. Card access controlled revolving doors or portals that permit one person at a time into the facility while simultaneously providing an audit trail.

3. Use of key pads requiring a Personal Identification Number (PIN) in conjunction with biometrics.

Where possible, parking should be located at least 50 feet from the perimeter of the building. Avoid facilities with underground or under-building parking. Facilities with uncontrolled/unmonitored underground or under-building parking that are not controlled (e.g., via card access controlled hydraulic gates or crash-resistant arms, card access controlled garage doors, on-site security guards dedicated to parking control, etc.) are not acceptable.

Security cameras must cover the primary entranceway to the lockbox facility, loading docks and surrounding areas, freight elevators and surrounding areas, parking areas, security guard stations that control parking lots, truck delivery areas, mail-sorting areas, mail extraction areas, and doors entering/exiting the general lockbox processing floor.

Trash, newspaper, mail receptacles, and unnecessary materials or equipment shall not be located within 50 feet of the building, thus eliminating the opportunity to conceal explosive or incendiary devices.

1. Where possible, parking should be located at least 50 feet from the perimeter of the building. Avoid facilities with underground or under-building parking. Facilities with uncontrolled/ unmonitored underground or under-building parking that are not controlled (e.g., via card access controlled hydraulic gates or crash-resistant arms, on-site security guards dedicated to parking control, etc.) are not acceptable.

2. Public/employee parking shall not be allowed in the loading dock area.

3. Signage for the building, parking stalls, or on the building directory should not include any words indicating that the QLP performs government financial operations.

4. Exposed exterior ladders/fire escapes shall not be available on the exterior of the building.

Trees must not allow accessibility to the building structure (e.g., roof, decks, and terraces).

Facility Security Plan: A facility security plan prepared in accordance with the prescribed Financial Management Service (FMS) format is required for each QLP facility and must be updated annually (see Attachment H on FMS' Web site www.fms.treas.gov/rebids/attachments).

Facility Blueprint: A blueprint of the facility, specifically processing floors and ground floors where main lobbies/entrances to the facility and loading docks are located, must be at least 2 feet (width) x 3 feet (height) in size and contain all security equipment (i.e., motion sensors, door alarms, emergency door exits, glass break sensors, cameras (interior and exterior), card readers, fire alarms, intercom systems, CCTV monitors, security guard stations, turnstiles, etc.). The blueprints should indicate the location and orientation of all cameras, and all security equipment should be numbered. The naming activity and numbers for security equipment should be consistent with naming activity and numbers reflected on CCTV monitors, camera numbers reflected on multiplexers, and with information used by the central monitoring station. Facility blueprints must be updated annually and submitted to FMS. Blueprints must be professionally prepared and reflect all processing work areas.

4.10.2. General Lockbox Perimeter

Secured Space

General lockbox processing shall be conducted in a secured space. Secured space is designed to prevent undetected entry by unauthorized persons. The following minimum standards must be met to qualify as secured space:

1. Surveillance camera coverage of entrances/exits to the processing floor, mail sorting/mail extraction areas
2. Security guard coverage
3. Intrusion Detection System (motion detectors, door alarms, glass break sensors)
4. CCTV monitoring

General lockbox extraction processes shall not be co-mingled with non-government extraction processes in the same space. Government incoming mail shall be segregated from corporate mail and other non-government media prior to extraction. Government mail shall be extracted in a dedicated room that meets the following minimum physical security standards:

1. Card reader on doors to track access
2. Surveillance camera coverage (interior and exterior)
3. Intrusion Detection System (motion detectors, door alarms)
4. Motion detectors to trigger room lights

Intrusion Detection System (IDS)

To detect attempted breaches into secured space, all perimeter doors leading into the general lockbox processing area and designated government work space must be equipped with door alarms. Designated general lockbox processing areas located on the ground floor must have glass break sensors to detect intrusions through the windows. Motion detectors must be used throughout the secured space to detect unauthorized intrusion.

The IDS must have a power source able to provide uninterrupted four (4) hours of battery-powered backup in the event of a primary power failure. The back-up power source should be tested at least once each year. A test of all IDS equipment should be conducted once a year. A logbook or alternate method to record testing dates must be maintained to document test dates and results. The test results should be documented and readily available for FMS inspections.

Duress Alarms

Duress alarm switches should be hidden from the public eye but accessible to sensitive guards and appropriate personnel without raising suspicion. The duress alarm should be programmed to invoke an immediate 911 response and notification to cognizant central monitoring stations. When pressed, the duress alarm should annunciate in the on-site manager's office. The annunciation can be non-audible (e.g., flashing strobe light, dull vibration, etc.) so as not to draw attention to the alarm within the facility.

Duress alarm procedures should be developed and documented by each lockbox site. The procedures must include the guard's responsibilities during an emergency situation. Testing of these alarms must be conducted twice a year. A logbook or alternate method must be maintained to document test dates and results. Security guards performing interior/exterior roving patrols, or responsible for escorting bank management and verifying visitors at loading docks, freight elevators, or other areas must perform such duties with a portable duress alarm.

Automated Entry System (AES)

QLPs using an AES must develop and document procedures to ensure that inventories of proximity or swipe cards are maintained in order to provide audit trails and deter unauthorized access. All employee information should be entered into the database, which must remain current to preclude entry of unauthorized individuals. Functional personnel should be fully trained on system capabilities and usage. A database log must be established and maintained to ensure accountability for proximity/swipe cards inclusive of the name of the person who issued the card, name of the recipient of the card, date card was issued, and date card was terminated or deactivated. Bank management must review the logbooks on a monthly basis. QLP facilities will have twenty-four (24) hours to delete access privileges for an employee that has been terminated, resigned, or whose tour of duty (e.g., temporary or seasonal employees) has been completed.

QLP facilities that utilize swipe card or proximity card access control to maintain separation of government processing space from other areas are required to ensure proper accountability procedures are used to detect and deter theft of cards. The QLP cannot delegate the badge issuance and turn-in (activation/deactivation) process to security guards or other third parties. The QLP must perform the necessary oversight to ensure proper checks and balances are used.

Exterior Doors

All perimeter doors leading into the QLP facility restricted secure space, and doors that permit access to/from the perimeter of the facility must:

1. Be solid wood or metal, at least 1 ¾ inches thick (this pertains to electrical and telecommunication rooms only),

2. Have interior door hinges or exterior door hinges equipped with security pins to prevent removal of the door from the hinge,

3. Not have windows, vents, or louvers that may be removed from the exterior, allowing unauthorized access, and

4. Not have openings that will allow the incision of tools to open the door latch while the door is closed.

All perimeter doors and doors to restricted areas (e.g., dedicated government mail extraction room, computer room, etc.) must have a key-operated, mortised or rim-mounted deadbolt lock, double cylinder of five (5) or more pin tumblers, and a one (1)-inch throw, at minimum. Combination/cipher locks may be used during duty hours to control entry into a facility. **However, during non-duty hours, combination and cipher locks must not be used as a sole locking device.** If deadbolt locks cannot be installed, IDS must be installed to indicate unauthorized access into the space.

Key and Combination Controls

Keys and/or combinations must be controlled and issued only to persons having a need to have access to an area, room, or container. The number of keys or knowledge of combinations must be kept to a minimum. Keys that are issued to an individual employee must be kept with the individual and not left in unsecured places, such as desk drawers. Keys should be "off master" (in multi-tenant buildings). A key register must be used to inventory and account for all keys, by type of key and total number, inclusive of keys under security guard control. Keys issued to individuals must be properly signed out using the key control log. The QLP is responsible for reviewing the key control logs monthly. The QLP is also responsible for conducting semiannual inventories of the key register to reconcile keys signed out according to the key log, with keys on-hand. All keys under the QLP control must be secure using a locked key box. Combinations to cipher door locks, safes, locks, and alarm systems must be changed:

1. When the safe or lock is originally received,
2. At least once a year,
3. When an employee who knows the combination retires, terminates employment, or transfers to another job/position, and
4. Whenever the combination is compromised.

At a minimum, combinations to cipher door locks, electronic locks (e.g., omni locks, etc.), safes, and alarm systems must be comprised of four (4) or more digits, and individually signed for to ensure accountability and for tracking, monitoring, and proper controls. Temporary combinations given to visitors must be issued using a log to ensure the visitor signs for the combination. Combination logs should be reviewed by bank management weekly, and bank management should deactivate combinations immediately upon the conclusion of the visitor's tour of duty or departure from the facility.

Surveillance Equipment

Specific requirements for surveillance cameras are as follows:

Mail Sorting and Mail Extraction: Surveillance cameras must allow management to view all workstations and activities in all mail-sorting and mail extraction areas (inclusive of certified mail extraction areas). Pan, Tilt, Zoom (PTZ) cameras must be used, and can be augmented by fixed cameras.

Loading Dock: Surveillance cameras must allow for complete coverage of the loading dock area (i.e., all bays, doors, points of approach). If security guards are assigned to sign in and badge vendors at the loading dock, this area must also be covered.

Freight Elevators: Surveillance cameras must be used to provide coverage of freight elevator doors and surrounding areas.

Video Tape Retention

The following guidelines apply for image retention:

1. Videotapes or other forms of image retention should be maintained by the lockbox for a minimum of six (6) months after the date of the tape's last annotated creation. After six (6) months from the date the tape was created, the tape can be destroyed or reused.

2. Tapes must be safeguarded in a locked container. Recording equipment must be secured at all times to prevent tampering. Access and usage must be limited to specific bank officials only.

4.10.3. Information Protection

The use of security containers or appropriate file cabinets to provide minimum protection standards is required for Privacy Act information, which includes incoming mail that has not yet been distributed or processed, negotiable instruments and related documents (e.g., checks, money orders, and related forms), as well as computer cartridges.

Items that require a higher level of security are listed below. These items must be controlled and stored in containers to prevent theft and fraud.

1. Currency
2. Key/key cards
3. Alarm and lock combinations
4. Passwords
5. Date stamps

Access to employee privacy information and assets that should be protected must be limited to select authorized bank employees only.

4.10.4. Lockers

Lockers may be provided for permanent bank employees, temporary lockbox employees, contractors, and Treasury employees to store personal belongings. Lockers must be located outside of the controlled work areas.

4.10.5. Badges

Anyone who enters the general lockbox processing area must wear an identification badge issued by the guard on duty. **These badges must be worn above the waist at all times**.

All QLP associates must have a unique ID swipe card that provides access to work functions within the processing area. Associates must display their ID cards at all times. **No associate will be permitted in the processing area without displaying his or her ID card**.

4.10.6. Security Equipment

Surveillance Cameras

Surveillance camera coverage strategically positioned to monitor perimeter doors leading into the facility, all doors that allow entry/exit to and from the general lockbox processing floor, loading dock areas, freight elevators and surrounding areas, security guard stations, mail-sorting areas, mail extraction areas, and check imaging/data processing areas (e.g., computer rooms) is required. PTZ cameras are required for mail-sorting and mail extraction areas, but could also be used to provide coverage of emergency exits, other sensitive areas on the processing floor (areas with a high susceptibility to identity theft or document theft/compromise), or to augment fixed

camera coverage. Surveillance cameras are crucial to performing the necessary monitoring, observation, and recording of events associated with the processing of government remittances. PTZ cameras must be programmed and pre-positioned to support alarm call up in response to emergency exit doors and other designated entry/exit doors. All interior and exterior cameras must be in protective, tamper- proof domes. Cameras must be capable of monitoring both normal and low light situations. Per-camera resolution shall be a minimum horizontal 400 lines.

Monitoring and Recording Equipment

Recording Equipment: QLP sites are required to record surveillance using digital video recording (DVR) systems using DVR multiplex recorders. The DVR system must be supported by the necessary peripheral security equipment to ensure effectiveness and compatibility. Video cassette recording (VCR) technology including the use of VCR tapes is not acceptable. Time-lapse recording is permitted provided that the time lapse does not exceed two seconds. When lockbox personnel are present, DVR recording must be on and activated. When lockbox personnel are not present, DVR recording must be either continuous or event activated. Event-activated recording means that activity such as an unauthorized breach into facilities and/or secured space is detected by IDS systems and triggers DVR recording. If event-activated recording is employed, all DRV recording must be conducted in real time.

Closed Circuit Television (CCTV) Monitoring Equipment: CCTV monitors must be large screen monitors capable of showing multiple cameras simultaneously (i.e., split screen, quad screen (quad splitters), multi-screen viewing). All monitors must produce a sharp, high-resolution picture of exceptional clarity. The horizontal resolution must be 600 to 700 lines at center. CCTV monitors must be located where they can be viewed by security guards (i.e., security guard stations). CCTV monitoring equipment and associated wiring should be checked twice annually by qualified security technicians. Automatic switchers and sequencers should be used to ensure CCTV monitors are capable of automatically switching to cameras in the area of activity/emergency, and have the ability to hold a scene on the screen or manually override the automatic action and select a specific camera. Monitoring and recording equipment must be supported by matrix and sequential switchers.

Intercom/Camera Devices

The use of combination intercom/camera device(s) is essential to effective physical security and access controls. An Aiphone® is an example of a combination intercom/camera device. Such a device allows an employee or security guard to perform critical validation and verification tasks prior to granting access to the facility and/or general lockbox processing floor area. It is imperative that facilities be equipped with such devices at key points of ingress, in order to (a) identify an individual and (b) to inspect the individual's identification, prior to permitting access to the facility and/or to sensitive areas. The use of substations is also a benefit since this configuration permits visual and verbal communication with multiple employee users such as between the receptionist, main guard station, and loading dock entrance. Since lockbox facilities vary (e.g., stand-alone versus multi-tenant facility) placement of these devices will vary.

Examples of placement areas include, but are not limited to, main entrances, employee entrances, loading docks, and gated situations that are designed to control vehicular traffic.

All security equipment must have four (4) hours of UPS/battery back-up to ensure continued operations until the alternate source of power is initiated.

Computer operations: The computer operations must be in a secure area. Non-related activities must not be located within the computer space. Environmental and housekeeping standards must be developed and maintained. Fire suppressant equipment, such as sprinklers, fire extinguishers, and fire suppressant trashcans should be utilized.

Access to computer operations must be limited to authorized employees and visitors.

A sign-in/sign-out log must be established and maintained. Each visitor entering the area must sign in and out on the log. An authorized QLP employee must escort visitors, whereas temporary employees will not be permitted into the area.

Separation of domains: QLP security equipment and controls, telecommunication equipment, and computer equipment must be located within the general lockbox space; each must be stored in separate rooms. Equipment and utilities must be locked to prevent tampering. Keys will be controlled and limited to authorized bank employees.

4.10.7. Access

Temporary Employees

Registration: Temporary employees must surrender current valid government-issued photo identification to the QLP prior to the issuance of an ID badge and access into the general lockbox processing area(s). The term "current, valid government-issued photo ID" should include the following forms of identification: a valid Motor Vehicle Administration (MVA)-issued driver's license, non-driver license issued by MVA, military ID, passport, or a lawful permanent resident alien card.

Note: The use of identifications such as a store card (e.g., Sam's Club card), credit cards, or other forms of identification issued by non-government institutions do not meet the requirements of government-issued photo identification and could lead to compromises and unauthorized access if accepted. The ID badge must be returned at the end of the shift in exchange for the temporary employee's photo ID. A copy of the employee's ID card must be maintained in the temporary employee's file.

All temporary agency personnel will only be permitted to access the site through one door located in the building. Badges must be returned at the end of the shift. An audit must be conducted at the end of each shift to ensure that all badges are accounted for. Identification media equipment and supplies must be stored in locked containers at all times to prevent theft and tampering.

Visitors

Only authorized visitors will be allowed access to the lockbox facility. Authorized visitors must provide proper identification; surrender current valid government-issued photo identification, and sign in with the security officer. Visitor logs must be maintained for 2 years starting with the date of the last entry.

Bank Officials and Official Visitors

Only QLP officials that have successfully completed the personnel security background investigation requirements contained in sections 4.10.15. through 4.10.20, and are responsible for lockbox duties, will be allowed unescorted access to the lockbox facility upon displaying the appropriate bank identification. All other QLP officials must provide a QLP-issued photo identification badge and sign in with the security guard. Bank officials must display their photo identification badge at all times. Official visitors are required to display their individual identification badge or obtain a bank-issued visitors badge that must be displayed at all times. No QLP official will be permitted in the processing area without displaying his/her photo identification card. QLP officials who have not successfully completed government personnel security requirement must be escorted at all times by a cleared employee.

Government Officials

Only government officials on the official contact listing will be allowed access to the lockbox facility upon authentication of the individuals' identity. Authorized government officials must provide a Federal government-issued photo identification badge and sign in with the security guard. Authorized government officials are exempt from the disclosure statement requirement. Government officials must display their photo identification card at all times. No government official will be permitted in the processing area without displaying his/her photo identification card. If possible, a temporary swipe card will be issued for the duration of the visit. Government officials on the official contact list do not require an escort. Any visiting government official who is not on the official contact list will be required to surrender a valid government-issued photo identification, sign in with the security guard (with the exception of FMS security review team members), and be escorted at all times.

Inspection Personnel

Special Agents and other auditors representing the investigative and program review functions of the U.S. Treasury Office of the Inspector General (OIG), respectively, should be granted staff-like access after proper authentication of IDs by the FA. The OIG, per the Inspector General Act of 1978, should receive full cooperation of the QLP in support of the OIG's broad investigative and audit powers related to (a) determining whether programs are achieving intended results and in compliance with governing laws and regulations, and (b) identifying fraud, waste, and abuse.

This is applicable to other government auditors (e.g., General Accounting Office) and/or their designated independent audit agencies or firms.

Emergency Personnel

Emergency response personnel are exempt from personnel background requirements contained in this document. To the greatest extent possible, these personnel should be escorted by QLP management personnel; however, in the case of an extreme emergency situation QLP management should ensure all data being processed is secured in an appropriate location.

Emergency personnel may include but are not limited to building guards, firefighter personnel, fire marshals and rescue personnel, FBI personnel, medical professionals, and law enforcement personnel.

4.10.8. Security Screening and Oversight

The QLP will provide adequate security, equipment, and facilities to safeguard all remittances and associated information received, processed, and mailed out of the facility as follows:

1. Lunch bags/boxes, purses, handbags, backpacks, briefcases, sports/duffel bags, notebooks, planners, baggy clothing (carpenter pants or oversized shirts) or bulky outerwear, hats, shopping bags, or any item similar to any of the aforementioned are not permitted in the areas where remittances are processed. Light jackets and sweaters may be worn in the remittance processing area if climatic conditions warrant. This requirement applies to everyone entering the processing area, including vendors, visitors, bank officials, and authorized government employees.

2. In the event that a vendor needs to enter the processing area with work-related items (e.g., tool kits, repair apparatus, testing equipment, manuals, etc.), the security guards must conduct a thorough search of these items before the vendor is allowed to enter or exit the processing area and escort the vendor at all times on the processing floor.

3. Food and beverages (those not in spill-proof containers) will not be allowed at the workstations.

4. Employees must be required to wear proper identification badges.

5. Access to sensitive work areas must be restricted.

6. Remittances will be controlled and secured between the source of receipt (post office) and the completion of processing the mail-out packages.

7. FMS will perform on-site security reviews to determine the effectiveness of security controls and compliance with this IEI. The security reviews will be performed normally in conjunction with the bank personnel, and may include the seeding of cash

or checks.

8. Date stamps used by the QLP must be safeguarded against unauthorized use.

4.10.9. Courier Service

All courier service contracts are negotiated between the QLP and the courier service. QLPs should ensure that couriers that are utilized are bonded. QLPs have the option of utilizing internal personnel for courier services; however, these personnel must be designated as such in writing and adhere to those applicable rules outlined below:

Packaging requirements: Privacy Act information, including checks, must be packaged for transmission in a manner that prevents unauthorized observation of Privacy Act data, loss, theft, or altering of documents or information. Government data should be transported in secure, locked tamper-proof containers.

The courier must reject shipments containing any opened, untagged, or unsealed packages and must allow the QLP 20 minutes to repair or replace the packaging.

Courier service driver procedures: Courier service must:

1. Adhere to policies and procedures required to transport government materials,
2. Wear a company uniform or be a permanent employee of the lockbox facility,
3. Be equipped with telephone/communication equipment,
4. Travel in pairs,
5. Be bonded or insured for $500,000, and
6. Carry the courier's identification card.

Disaster contingency plan: Prior to implementation of the contract, the courier service must provide the QLP with a disaster contingency plan. The contingency plan must cover labor disputes, employee strikes, inclement weather, natural disasters, traffic accidents, and unforeseen events. This plan should be reviewed and appropriate upgrades documented at a minimum of once per year.

Notification: The courier service must immediately notify the QLP when established timeframes cannot be met. The courier must also notify the QLP within one (1) hour of accident or the theft and/or destruction of government property being transported. To ensure this notification is made promptly, vehicles must contain appropriate depositary contact numbers and radio or telephone communication equipment within the vehicle. The courier service must also provide to the depositary an updated list of employees who will be assigned to the depositary during the term of the contract. This must be accomplished annually on or about October 1.

Contact information: Upon contract implementation, the courier service must provide the QLP with two (2) contact names (a primary and an alternate), telephone numbers, and pager numbers,

if applicable. At the same time, the courier service must also provide the QLP with a 24-hour emergency telephone number and name of the person to contact during non-business hours.

The courier service must notify the QLP within 24 hours of any change in contact persons and/or telephone numbers.

Courier service employee information: Upon contract implementation, the courier service must provide the QLP, on official letterhead, the following information for each employee assigned to the QLP courier contract:

1. Employee name,
2. Title,
3. Signature,
4. A valid driver's license, and
5. Photograph of each employee assigned.

The courier service must notify the QLP within 24 hours, via facsimile transmission, when an employee assigned is discharged from his/her duties. The courier service must also deliver the identification information to the QLP prior to assigning the new employee to any route. The courier service must also notify the QLP within 24 hours, via facsimile, of the hiring of new employees assigned to the contract.

The courier service must provide each employee assigned to the contract with company photo identification. The company photo identification must contain the following employee information, consistent with what has been provided to the QLPs:

1. Employee name,
2. Employee signature,
3. Company name,
4. Company officer signature,
5. Expiration date,
6. Identification number, and
7. Photograph.

The QLP should maintain files containing a copy of each courier's driver's license and company photo identification. Procedures should be developed and implemented to ensure proper validation of courier drivers' identification.

On-duty couriers: All courier personnel must display (on their person) the company-issued photo that clearly identifies the individual as authorized messenger for the courier service. Company logo uniforms are required for all courier employees assigned to the FA contract.

Vehicle requirements: The courier vehicle being used to transport government data and/or remittance data must always be locked and secured whenever government data are contained within the vehicle until it reaches its destination. The vehicle must always be under the

supervision of one of the couriers and never left unattended while transporting or containing government packages or containers.

Shipment transport requirements: The following must be adhered to during transport:

1. Vehicles used by the courier must be maintained in good condition, appearance, and working order. The vehicle must meet the minimum safety standards of the state in which each vehicle is operated.

2. Vehicles used by the courier must be enclosed to ensure the packages or containers carried by the vehicle are secure. No open vehicles (pickup trucks with open beds, vehicles with glass camper tops or no doors, motorcycles, etc.) may be used to transport packages/containers.

3. Vehicles must be secured (doors closed and locked) during transportation of the package or containers. Vehicle doors must be able to be secured from both inside and outside.

4. To avoid lost documents, packages must be sealed and containers locked.

5. When possible, packages must be placed in fire-resistant containers.

6. Once the vehicle is in possession of the government's packages or containers and the doors are locked, the doors must not be unlocked until the vehicle has arrived at its destination.

7. Upon arrival at the designated site, the driver must remain with the packages/containers until they are unloaded at the receiving site.

8. Upon delivery of the packages/containers to the designated site, the driver must obtain a signature of the person receiving the material and annotate the time of the delivery.

9. Couriers must promptly notify the QLP when packages/containers cannot be delivered within the established timeframes due to accident, vehicle disablement, robbery, or any other unforeseen event.

10. The QLP must maintain a log showing the courier driver's signature, date of pickup, number of boxes, and time of pickup.

11. QLP management must review the logs mentioned above on a monthly basis.

QLPs involvement: The **QLP** reserves the right to inspect vehicles and personnel involved in courier operations to determine compliance with applicable requirements.

4.10.10. Guard Services

Overview

Guards are an important element in the overall security plan, and the functions they perform must be related to all other elements of the plan. The image of a well-trained, uniformed security officer is an asset that serves not only to deter crime, but also to promote an environment in which employees will feel secure and safe.

When QLP personnel are not present, guards are not required. However, when guards are not present, the facility should be secured and intrusion detection systems fully activated. When personnel are present, the minimum guard requirements are as follows:

Commercial, multi-tenant facilities must have security guards to perform access control duties, monitor personnel entering the facility (e.g., main lobbies, entrances designated for "employees only") and personnel reporting to loading dock/delivery areas. In cases where general lockbox processing is performed in a facility that does not have security guards located at main lobbies, loading dock areas, or other common areas to monitor access controls, the QLP must have acceptable access control measures for entrances to the facility as identified in Section 4.10.1 and dedicated security guards and a supporting security guard station on the general lockbox processing floor. There must be a minimum of two (2) guards on site per shift (one guard at all times at the entrance to the general lockbox processing area and one (1) rover guard). Trained law enforcement or security personnel who are dedicated to performing such duties must perform security guard duties. Security guard duties are not administrative duties and thus cannot be performed by unqualified personnel (e.g., bank associates, temporary hires, etc.).

Security guards must be assigned to a security guard station or designated guard posts. The security guard station must be equipped with CCTV monitoring equipment, duress alarms, land line telephone, internal communications (e.g., two-way radios), and post orders. Secondary guard posts should be equipped at an appropriate level that guards can perform effectively. Security guards must be required to physically touch each badge to verify the legitimacy of the badge and to match the badge photo with the face of the presenter.

Guards assigned to the facility (i.e., are not dedicated to the general lockbox processing area) are not subject to the personnel security requirements contained in Sections 4.10.12 through 4.10.23 (Personnel Security Requirements); however, it is expected that these guards undergo background checks in accordance with corporate policy. Dedicated security guards assigned to the general lockbox processing floor, however, are subject to the personnel security and background check requirements contained in Sections 4.10.12 through 4.10.23.

Functions

The basic functions of security guards are to respond to and report incidents; monitor and observe activity on the processing floor; uphold applicable security requirements; detect and deter theft, fraud, waste and abuse; monitor material and personnel coming into and going out of

the processing area; maintain guard logs of activity and incidents; and report suspicious or unusual activity. Security guard master logs must be maintained for 2 years from the date of the last entry.

Closed Circuit Television (CCTV) Monitoring: Guards must be properly trained in the use, capability, and purpose of surveillance equipment in order to operate and monitor CCTV systems. Security guards are responsible for monitoring CCTV activity to (a) observe critical/sensitive areas (e.g., entrance(s), mailrooms, extraction areas, etc.), (b) detect unusual activity and/or unsafe practices, and (c) provide early warning of possible security compromises and attempted compromises. The location of security monitors must be within proximity to security guards to permit observation of areas (internal/external) designated by the QLP as critical areas.

The responsibility for CCTV monitoring by security guards should be done on an ongoing (active) basis and whenever guards are not engaged in performing another security duty (e.g., signing in a visitor, badge issuance/ID exchange, escorting bank management to the loading dock to receive mail, or other security duties, etc.). Active monitoring does not mean 24-hour continuous CCTV monitoring by a guard. Additionally, security guards perform the following functions: (a) monitor the extraction area; (b) staff the front desk/entrance into the processing area; (c) patrol the perimeter; and (d) perform emergency response duties. When QLPs rely on security personnel other than a dedicated guard force, QLP management must ensure a designated trained bank security official conducts active CCTV monitoring.

Post orders: Post orders provide security policies and summarize required guard duties. They also avoid the inherent problems in word-of-mouth instruction that can be forgotten or misunderstood. Post orders should be specific for each major function the security guard must perform. For example, a separate set of post orders should be developed for guards posted on that entrance area versus roving guard orders. Post orders should be developed with the following criteria in mind:

1. Post orders must be relevant to the unique operational settings and physical design of the facility. Post orders must be specific to the operations and associated vulnerabilities specific to the location and processes at the site.

2. Each order must deal with one subject, permitting the guard or management to locate a policy or procedure rapidly when consulting with orders.

3. Each order must be as brief as possible. The order is an action document stating clearly what is to be accomplished and when. It should not include narrative justification for the order.

4. Each order must be written in simple terms that can be easily interpreted.

5. Each order is indexed to permit ready reference.

Patrol: Patrols can be performed either on foot or in a vehicle. Intermittent patrols of the perimeter of the facility (inclusive of parking lots, checks of perimeter doors, trash dumpsters, generator areas, etc.) shall be conducted and accounted for in the security guard's log. Items that must be checked and, thus, included in the officer post orders include:

1. Doors, windows, or other openings that are not locked,

2. All suspicious persons, vehicles, boxes/packages, or circumstances,

3. Indications of disorder, excitement, or unusual activity, and

4. Hazardous conditions, such as water leaks, unlocked rooms containing dangerous substances, fire hazards, and malfunctioning equipment.

Escort: Guards may be utilized to escort visitors and customers; however, it is usually the responsibility of the individual being visited to provide the escort. Guards may also escort those who need assistance due to illness or physical disability.

Incident reporting: This is a key responsibility for the QLPs and, in particular, the security guard force. The report should answer the following questions:

Who was involved? The guard should give a complete description, including names and titles, if appropriate,

What happened? This does not mean what could have happened, or what someone thought might have happened,

Where did the incident occur? To alleviate confusion, the description of where the incident occurred should be clearly identified,

When did the incident occur? The specific timeframe (including date and hour of the incident), and

Why did the incident occur? This is significant when intent is an element of the incident. The facts must be stated and the guard(s) must not include their own opinions.

Examples of reportable situations include, but are not limited to:

1. Natural disasters, such as earthquakes, flooding, and hurricanes,
2. Fires and explosions,
3. Bomb threats or attacks,
4. Arson,
5. Chemical threats or attacks,
6. Biological threats or attacks (including all "white powder" discoveries),
7. Radiological threats/terrorist acts,

8. Cyber attacks,
9. Threats of violence against employees or the facility,
10. Information technology/equipment failures,
11. Workplace violence (if a 911 call is necessary or business is disrupted),
12. Civil disorder/demonstrations,
13. Weather-related closings or delays, such as severe ice or snow,
14. Theft (of checks or sensitive information),
15. Loss,
16. Unauthorized disclosure,
17. Unauthorized entry that created significant impact on operations or safety of employees,
18. Unauthorized shredding of government media,
19. Staffing or security problems, which cannot be mitigated immediately and threaten attainment of minimum daily processing or compliance with applicable security requirements, and
20. Any other critical events or events of such an unusual nature that immediate notification is required.

The bank must maintain a log of incident reports, noting corrective follow-up actions taken on each incident.

FMS must be notified within 30 minutes of an incident. A clear, concise, and factual report (via the Event/Incident form), answering the above questions, must be e-mailed and/or faxed to FMS within 24 hours of the incident.

Issuance of weapons: If an armed guard force is used, the guards must be properly trained and certified in the use of firearms. The firearm is to be drawn as a last resort—only in a defensive situation for the protection and defense of life. The firearm must never be left unattended, even momentarily. Aside from the competency of the guard, the following major policy considerations should be reviewed:

1. The conditions under which the weapon may be issued,
2. The accountability maintained over the weapon and ammunition,
3. Legal restrictions covering issuance and usage,
4. Clearly written instructions as to the circumstances in which weapons may be utilized,
5. Safety precautions surrounding the issuance and carriage of weapons, and
6. Secure storage for weapons and ammunition when not in use (if applicable).

Minimum Guard Coverage Requirements

Commercial, multi-tenant facilities must have security guards to perform access control duties, monitor personnel entering the facility (e.g., main lobbies, entrances designated for "employees only") and personnel reporting to loading dock/delivery areas. In the event guards are not present at the facility to perform access control duties, the general lockbox processing sites must

have two (2) security guards (one fixed post and one rover) assigned to the processing floor at all times during hours of operation. When the facility is closed, the Intrusion Detection System (IDS) can suffice to provide security after hours of operation.

Main entrances and loading docks are required to have security guard coverage during business hours and after business hours if IDS is not available. QLP facilities may employee dedicated security guard personnel or utilize security guard personnel provided for building protection when the lockbox facility is a tenant in a host building.

Security Guards – Access Control

A primary function of the guard is to permit authorized persons into a facility and/or the lockbox-processing floor, and at the same time keep unauthorized persons out.

Post orders given to the guards must include the following procedures:

1. Ensure that all employees wear a badge above their waists. The badge must be visible at all times while in the processing area.

2. Identify all visitors and issue special badges to them after the escort reports to the security guard station, verifies that the visitor has legitimate business at the facility, and signs the visitor's logbook.

3. Provide sign-in/sign-out control for all visitors. Visitor logs must be maintained for 2 years starting with the date of the last entry.

4. Report any person in the facility without authorization to management.

5. Report individuals who bring liquor or other contraband into the facility or who are under the influence of liquor or drugs.

6. Question individuals who attempt to remove property from the facility.

7. Check all property removed from the facility to ensure that the individual has a valid property pass.

8. Inspect all incoming packages and mail deliveries.

9. Ensure that all boxes, packages, and courier vehicles are not left unattended in the loading area.

10. Escort the mail-out process for packages being picked up for delivery to the service center.

11. Inspect all personnel and materials leaving the processing floor (this includes

inspecting all papers, documents, and other items for theft of checks, Privacy Act information, and other unauthorized data).

QLP management is ultimately responsible for access control procedures and accountable for ensuring that only authorized personnel are granted access to the processing floor. Bank management must be involved in the day-to-day access control process. This responsibility cannot be delegated (e.g., to temporary agency personnel, security guards, third parties, etc.)

Inspections: QLP management must monitor the guard contract to ensure that all officers are properly trained (including certification of firearms proficiency), attired, and executing their duties. Also, QLP management must maintain reports of inspections.

4.10.11. Security Awareness Program

An effective security awareness program must include the following as a minimum:

1. All new permanent and temporary QLP employees must go through a security orientation within 10 business days of arrival to the processing location. Before allowing employees to access Privacy Act information, employees must certify that they understand security procedures and instructions requiring their awareness and compliance. The initial certification and annual recertification of security awareness training should be documented and training attendance records validating the employee/temp hire attendance placed in personnel Treasury files. The annual recertification for security awareness training must be conducted between January and March of each year. This certification must be documented and made available for FMS inspectors upon request.

2. Managers may use an after-hours review as an additional tool to assess employee awareness and security practices.

3. A variety of methods may be used to disseminate security information and requirements: formal and informal training, group meetings, bulletin boards, employee newsletters, and posters. Documentation of such activities shall be presented upon request to QLP representatives during on-site security reviews; however, these informal methods of communicating security matters to ensure employee security awareness are not a substitute for the mandated formal security awareness training that is required within the employees' initial entry into the lockbox facility and annual recertification.

4. Procedures for handling suspicious packages or suspected contaminated mail situations must be distributed and posted in the mailroom.

Occupant emergency plan (OEP) and safety precautions: An OEP must be developed and updated annually. At minimum, the plan should contain a call list for emergencies, as well as procedures to address bomb threats, fire, evacuation, severe weather conditions, natural disasters (e.g., earthquakes, tornadoes, etc.), demonstrations and civil disorders, and procedures to ensure

disabled employees are cared for during such emergencies (see Attachment I on FMS' Web site www.fms.treas.gov/rebids/attachments).

A fire drill should be conducted at a minimum of once a year. Fire extinguisher locations throughout the space must be clearly marked and extinguishers inspected by the local fire department annually. Upon request, proof/certification that the facility has passed inspection should be provided to FMS and/or QLPs.

The bank should exhibit good housekeeping and follow general safety practices. Hazardous, combustible materials, as well as smoking, may not be permitted in the facility. Computer equipment should be placed away from obvious risks, such as water pipes. Cartridges should be protected from magnets, liquids, and other hazards.

4.10.12. Personnel Security

4.10.13. Personnel - Employee

The following personnel security requirements apply to any individual that has staff-like (i.e., unescorted) access to lockbox facilities, and/or any individual that handles/processes lockbox media (remittances/information).

4.10.14. Personnel Scope

Error! Bookmark not defined.
The extent to which an individual is considered an employee within a general lockbox system is broad and applies as follows:

> Any QLP employee, including, but not limited to, full-time, part-time, temporary, or seasonal workers, as well as all contractors and vendors that transport, process, sort, extract, image, secure, or in any way handle lockbox media inclusive of managers and supervisors that are responsible for oversight, and
>
> QLP employees with staff-like access to general lockbox processing floors, information systems, and/or sensitive but unclassified information.

These requirements apply to the security guard force if such a force is dedicated solely to the general lockbox. These requirements do not apply if, in addition to the general lockbox, the guard force is also charged with protecting a commercial, multi-tenant facility.

4.10.15. Employee Eligibility

Consistent with Title 12, United States Code, Section 1829, no person shall work or have access to lockbox facilities and/or lockbox media who have been convicted of criminal offenses involving dishonesty, breach of trust, or money laundering. Outside of these requirements, the QLP has the flexibility to hire and maintain individual employment; however, QLP officials shall consider, weigh, and investigate results and verifications that are obtained through initial background screenings, employee-submitted documentation, and periodic reinvestigations.

Employee Verification Service (EVS)

This is a free screening that can only be cleared through the Social Security Administration (SSA). SSA will advise the requesting employer whether an employee's name and Social Security number (SSN) matches SSA records. A non-match does not imply that the employee intentionally provided incorrect information about his/her name or SSN. Once a successful match is made via EVS, no periodic reinvestigation is necessary since EVS is not a security-designated service. If there is a non-match, the employee must be given reasonable time to visit

the local SSA office to correct any discrepancy, and appropriate follow-up via EVS must be completed by the FA. SSA provides guidance to all employers that use the EVS service, and financial agents are expected to comply with EVS guidelines.

4.10.16. Background Investigation

Screenings: Personnel security screenings must be completed and adjudicated prior to deeming an employee eligible or permitting unescorted access to lockbox facilities and/or the handling of lockbox media for the Federal government. Two separate levels of screening are outlined—Baseline and Standard.

Baseline Screenings: Baseline personnel screenings apply to all individuals with staff-like access to lockbox information and facilities. At the discretion of FMS, baseline screenings may serve as the sole investigative screening requirement contingent upon lockbox scope. In addition, certain contractors such as janitors, electricians, carpenters, photocopier/telephone repair vendors, and other facility maintenance personnel with staff-like access are subject to baseline screenings only.

1. FBI fingerprint check,
2. Local police check.

Standard Screenings: Standard personnel screenings are required based on job function, degree of staff-like access, and/or the sensitivity of the lockbox operation. Standard screenings include:

1. FBI fingerprint check,
2. Local police check,
3. Credit check,
4. Retail theft/fraud screening,
5. Social Security Number Trace.

Applying Standard Screenings: Within the lockbox environment, it is recognized there will be personnel with greater accessibility to government media by virtue of duties and/or lockbox operations. For example, standard screenings would be required for personnel with staff-like (i.e., unescorted) access including, but not limited to, full-time, part-time, temporary and seasonal employees, couriers, guards, and certain contractors such as unescorted systems repair and security technicians. Except in cases where the baseline screenings serve as the sole investigative standard, the standard screenings will apply. FMS will make the determination whether the standard screenings or baseline screenings apply to a particular lockbox cash flow environment on a case-by-case basis and communicate its decision in writing to the QLP.

4.10.17. Primary Screening Requirements

Adjudication: QLP officials are responsible for ensuring that primary screenings as outlined below are conducted and that screening results are investigated, weighed, and adjudicated, except as directed by FMS otherwise on a case-by-case basis. QLP officials shall conduct

screening result adjudications for suitability determinations using the criteria specified in IEI, Attachment J, Suitability Factors (see FMS' Web site www.fms.treas.gov/rebids/attachments.) If requested, QLP officials must also be prepared to defend to Treasury officials hiring decisions based on primary screening results.

FBI Fingerprints: This clearance must screen for felony/misdemeanor arrests and dispositions based on the subject's fingerprints. Fingerprints may be submitted to the FBI either electronically or by hard copy. If hard copy is used, two separate fingerprint sets must be made. One set is sent to the FBI for screening while the QLP must retain the other set. If fingerprints are submitted electronically, the QLP must make and retain a copy using an FBI-approved printer.

Local Police Check: Using a subject's self-reported seven-year address history, screen for felony and misdemeanor arrests and dispositions with each jurisdiction. Because civic norms vary, local police checks may involve clearing through courthouses, precincts, cities, counties, or states. (See also "SSN Trace" below.)

Credit Check: Obtain subject's financial history from a credit reporting agency (CRA) for the past seven years including liens, judgments, and bankruptcies. Make, justify, and document necessary hiring decisions based on subject's creditworthiness.

Retail Theft/Fraud History: A variety of private security vendors have access to past incidents of confirmed employee and customer theft against national and regional retail organizations. Such incidents are not often prosecuted or reported to law enforcement agencies; however, a restitution agreement, confession, or other evidence has been substantiated. Screening involves generally submitting a subject's name and SSN to a qualified vendor. The screening process must also comply with the Fair Credit Reporting Act, and the scope of screenings must include both regional and national retail organizations. Negative findings must be substantiated by appropriate evidence since an accurate "hit" shall disqualify the subject from employment.

SSN Trace: This process is multifaceted and involves authenticating information using a subject employee's SSN. Most private security vendors obtain this information through CRAs and possibly other sources. Fraudulent use of SSNs and identity theft is a growing problem, and this form of authentication is designed to detect fraudulent use. The SSN trace must include the following:

1. Authenticate that an SSN is associated with the subject (name of individual) and no one else including aliases, names of others using the SSN, and use of false numbers;

2. Authenticate that the subject's SSN, as issued by SSA, falls within a valid range based on verification of the year and state the SSN was issued in;

3. Authenticate that the subject's SSN was never issued or was/was not used in a death report or is part of SSA's deceased file record; and

4. Authenticate that the subject's seven-year self-reported address history is consistent with CRA records. Any discrepancies between the subject's self-reported address history and CRA information must be investigated (i.e., local police check).

4.10.18. Periodic Reinvestigation

Full-Time Employees: Any employee designated as full time, or maintains a regular and routine workweek of at least 35 hours, shall be subject to a periodic reinvestigation inclusive of having primary screenings refreshed every five years.

Part-Time Employees: Any employee designated as part time, temporary, seasonal, or lacking full- time status, shall be subject to a periodic reinvestigation inclusive of having primary screenings refreshed every three years.

4.10.19. Background Employee Documentation

Vital Information: As a condition of employment, and prior to staff-like access to lockbox facilities or media, the QLP must request and obtain original documentation directly from the subject. This documentation includes:

1. Proof of U.S. citizenship,
2. Lawful permanent resident status (if applicable),
3. Signed non-disclosure statement, and
4. Signed Rules of Behavior document.

Table 1: The table below addresses documentation that is required from the lockbox employees. How to treat this information, including maintaining and updating documentation, is also addressed.

Table 1: Primary Employee Documentation – Handling, Updating, and Verification

Source	Documentation /Updating	Handling/Verification
Employee	**Citizenship** Mandatory for initial screening. Only update/reinvestigate if situation warrants.	Review subject's original birth certificate, original U.S. passport, or original Naturalization documentation and retain photocopy. Lacking original documentation, contact appropriate civil authority to verify citizenship. Maintain any records/information related to verification.
Employee	**Lawful Permanent Resident** Mandatory for initial screening. Update if indicated (see handling).	Review subject's original documentation such as Form I-551 or "Green Card" issued by the Immigration and Naturalization Service (INS) and retain photocopy. If an expiration date is indicated, reinvestigate the subject's proper renewal or legal status at the appropriate time. Maintain any records or information related to verification.
QLP, signed by employee	**Non-disclosure Statement** Mandatory initial screening. Updated yearly thereafter.	Employee must agree and attest in writing to protect sensitive lockbox media and information from unauthorized disclosure. Statement must be signed and dated by the employee.
QLP, signed by employee	**FA Rules of Behavior**	Employee must agree and attest in writing to protect assets and transmissions related to government

		operations from unauthorized disclosure and uphold IT security principles and guidelines.

4.10.20. Additional Personnel Security Requirements

Treasury Folder: The QLP shall retain all initial background screenings and periodic reinvestigations, together with other documentation referenced in this section and in Sections 4.10.15. through 4.10.19. Personnel Security, in a separate folder for each employee. This folder, referred to as an employee's "Treasury Folder," must be stored in a secured space within the lockbox facility. Treasury Folders should be separate and apart from personnel records that contain private information related to job performance, salary, or other similar information. Employees must be made aware that all information contained in their Treasury Folder is subject to inspection and that information is subject to reinvestigation. Other documentation may also need to be stored in a subject's Treasury Folder, including, but not limited to, proof of security awareness training.

Tracking and Accountability: The QLP shall develop and implement an acceptable tracking system, approved by Treasury, that is designed to ensure that all required screenings, documentation, and verifications are in place, current, adjudicated, and refreshed in a timely manner.

Audit and Review: QLP employees and management should be made aware that that proof (or evidence) of background investigations, or information contained in an employee's Treasury Folder, are subject to inspection and review by appropriate Treasury officials. Appropriate QLP representatives, including lockbox managers and supervisors or those acting on behalf of same, agree to provide to Treasury officials, during announced and unannounced site visits, immediate and unencumbered access to Treasury Folders.

Digital Photograph: QLP officials must obtain a current, date-stamped retrievable digital photograph of the employee prior to staff-like access to facilities or lockbox media. The retrievable digital photograph must be dated within the last five years.

Handwriting Exemplar, Requested Specimen: The subject must provide a handwriting sample based on a QLP-provided exemplar once employment eligibility is determined. The sample must also be completed under the full and direct scrutiny of a qualified witness. Exemplar language needs to be developed by the QLP, and the sample language should be relevant to a lockbox environment (e.g., sample incident report). The exemplar must contain a minimum of two four-sentence paragraphs, include numbers, and also contain at least three stand-alone sentences that are printed (not written) by the subject. The subject must both sign and print his/her name on the exemplar and include the date. After initial completion, an exemplar must be refreshed every five years thereafter. Older exemplar versions must also be retained.

Records Retention: All screenings and documentation as outlined in Sections 4.10.15. through 4.10.23., that are contained in Treasury Folders must be retained for five years after separation or transfer. Except for handwriting exemplars and photographs/video image, most background

investigation reports (primary screenings) may be shredded and destroyed as earlier results are updated due to periodic reinvestigation requirements.

4.10.21. Employee Roster

Immediate Staff: QLPs shall maintain a roster of current eligible employees. Changes or updates to the roster must be annotated by date. When the QLP deems an employee eligible, the roster must be updated within 48 hours. Also, as employees resign or are otherwise deemed ineligible, names must be removed or disqualification annotated within 24 hours. Eligible employees include, but are not limited to, full-time, part-time, and temporary staff including managers, supervisors, and contractors who have completed the personnel security investigative requirements and deemed suitable. At a minimum, the roster must include the subject's name, job descriptor, date of eligibility, and, if necessary, date of ineligibility.
Vendors and Contractors: Vendors and contractors must also be included or addressed on a separate employee roster. QLP officials must ensure that vendors and contractors understand their responsibility to report changes in an employee's eligibility status within a timely manner (i.e., eligibility within 48 hours; ineligibility within 24 hours) in order to maintain compliance. At a minimum, the roster must include the subject's name, job descriptor, assignment on the processing floor, date of eligibility, and, if necessary, date of ineligibility.

4.10.22. Security Awareness Training

Initial and Annual Recertification: Any and all eligible employees must undergo security orientation by the QLP. Such an orientation must be conducted initially or before an individual has staff-like access to lockbox facilities and/or media and repeated at least annually.

FMS IT Security Policy: Any initial and annual refresher program shall be in accordance with FMS IT Security Policy 2.15, Information Technology Security Education and Awareness Training, for all personnel involved in the management, operation, programming, maintenance, or use of the lockbox system. QLPs and contractor employees shall be aware of the security responsibilities, know how to fulfill them, and know the penalties involved if they are not fulfilled.

Security Awareness Program: The QLP must demonstrate that an effective security awareness program is in place through practicing and demonstrating to Treasury that these minimum requirements are in place:

1. Each employee must certify in writing that they understand security procedures and instructions that require their awareness and compliance. This certification and annual recertification must be contained in the employee's Treasury Folder.

2. Employee completion of a non-disclosure statement, which is witnessed and completed in a controlled environment.

3. Bank management must ensure that employees are aware of the penalties associated with unauthorized disclosure even after their employment has ended.

4. Samples of security concerns that must be addressed include bomb threats, mail bombs, evacuation, incident reporting, and safeguarding facilities and media.

5. Address the consequences of fraud and inadvertent and willful unauthorized disclosure. Also address deterrent practices and procedures related to CCTV surveillance, seeding, theft, dress code, and the proper stowage of personal belongings.

6. Procedures for handling suspicious package situations must be addressed through training and also posted in the mailroom.

7. Procedures for reporting crimes, suspicious activities, or other incidents.

8. Procedures relevant to building and system security, which may include user codes, passwords, badges, building access, and intrusion detection.

9. Any other practice or procedure that will facilitate and enhance security awareness.

As part of the security awareness process, employees must be trained to protect lockbox media/information by:

1. Not discussing it with individuals who do not have a need-to-know,

2. Not discussing it in public areas where it could be overheard,

3. Ensuring all printed reports, documents, and other information are securely stored when not in use,

4. Ensuring printed documents and any diskettes containing information are properly destroyed when no longer needed,

5. Ensuring they either exit the system and log off or use a password-protected screensaver when they are away from their workstations for any length of time,

6. Ensuring they choose passwords that cannot be easily guessed by someone else, and

7. Ensuring only they know the passwords.

4.10.23. Exit Debriefing

Non-Disclosure: In addition to any other process or procedures relative to employment resignation or termination, the debriefing process must include guidance and signed statements, which outline penalties associated with unauthorized disclosure should the departing employee disclose information pertaining to lockbox remittances and associated data, privacy act

information, and any other sensitive but unclassified, programmatic, operational, and/or facility/security lockbox related information that they had knowledge of/access to. The departing employee must be made aware of their responsibility not to disclose information pertaining to lockbox operations.

4.11 Information Technology (IT) Security

Appropriate Security. In general, the QLP shall ensure that an appropriate level of information technology (IT) security, commensurate with the risks and threats, is established for General Lockbox Services.

FMS Entity-wide IT Security Program. To the extent that IT systems are employed to support General Lockbox Services, the provisions of the Financial Management Service's (FMS) Entity-wide IT Security Program apply, as identified in this section.

In general, standard commercial check clearing, sorting, settlement, posting, and accounting resources are not the types of resources that will be considered IT systems for purposes of General Lockbox Services.

In general, applications developed specifically pursuant to this IEI are the types of resources that may be considered IT systems.

FMS IT Security Manuals. To the extent that IT systems are employed to support General Lockbox Services, the QLP shall comply with all applicable elements of FMS IT Security Policy Manual and FMS IT Security Standards Manual (these manuals are available upon request).

Inquiries on FMS IT Security Manuals. During the bidding process, if the FI has a question about the applicability of an element of the Policy or Standards Manuals, inquiries may be directed to the General Lockbox Rebid Program Manager (see Section 3.1.1). After the DFA is signed, the QLP may contact FMS' Division Information Officer, Federal Finance for further clarification.

Certification and Accreditation (C & A). To the extent that IT systems are employed to support General Lockbox Services prescribed in this IEI, such systems must be certified and accredited in accordance with the following definitions, rules, and procedures, prior to processing transactions:

1. Certification is an evaluation process resulting in a judgment stating whether a system meets a specified set of security requirements. Systems may be certified at Levels 1 – 4 (as described later in this section under C & A Process).

2. Accreditation (also called *Authority to Operate*) is an official management authorization for a system to process data in an operational environment at an acceptable level of residual risk.

3. The QLP shall produce the following documents in support of Certification and Accreditation of any systems used to support General Lockbox Services:

System Security Authorization Agreement (SSAA). The SSAA is an agreement among the accreditor, the certifier, program manager, and user representative. This document is described in and should be tailored from, Annex A of the National Information Assurance Certification and Accreditation Process, available at http://www.nstissc.gov/Assets/pdf/nstissi_1000.pdf. The Division Information Officer, Federal Finance, FMS, will assist in defining appropriate SSAA tailoring.

Security Plan. The Security Plan identifies the security requirements of the system and whether appropriate technical, management, and operational controls are in place or planned. This document must include all security requirements, if necessary, by reference to other documents (e.g., security, functional or business requirements documents that contain security requirements). The Security Plan is defined in NIST Special Publication 800-18, available at http://csrc.nist.gov/publications/nistpubs/index.html.

Security Activity Checklist. The Checklist has been developed by FMS based on the NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, available at http://csrc.nist.gov/publications/nistpubs/index.html.

Contingency Plan. The Contingency Plan identifies the priorities, resources, and procedures necessary to ensure that essential operational tasks can be continued after disruption to a system. This document should address both continuity of operations and disaster recovery. This document is defined in NIST Special Publication 800-34, available at http://csrc.nist.gov/publications/nistpubs/index.html.

Configuration Management (CM) Plan. The CM Plan defines the identification, control, accounting for, and auditing of all changes to system hardware, software, firmware, documentation, test plans, and test results throughout the life cycle of the system. This document includes Change Control.

Security Concept of Operations (ConOps). The Security ConOps describes how all types of users, administrators, and external processes interact with the system, ensuring that security controls are understood and used correctly, to include how the system is to be configured and operated to maintain its acceptable level of risk. This document includes Incident Response and an Escalation Matrix.

Business Risk Assessment (BRA). The BRA evaluates the sensitivity of the information being used by the business process, identifies threats to the business process, and identifies the management controls to protect the business process. The end result of this assessment is the identification of internal controls (both manual and automated controls) needed to maintain the integrity of the business process as well as the identification of privacy, reliability, and availability requirements imposed on the process. This document may be drafted after both the business process model diagram(s) and the logical data flow diagram(s) are approved. This process is defined

in Technical Report – 2002-04, *Financial Management Service Business Risk Assessment: A Methodology* (this document will be provided upon request).

Technical Vulnerability Assessment Report (also called System Risk Assessment). This identifies existing and potential threats, vulnerabilities, and the effectiveness of the current and proposed safeguards, including technical, management, and operational controls described in the Security Plan. This analysis need not use automated tools or hands-on testing. This is to be accomplished by an independent third party approved by the Division Information Officer, Federal Finance, FMS. Note that this document covers *technical* risks.

Security Test and Evaluation (ST&E) Report. The ST&E states the findings, potential impact, and recommendations of the effort to verify that all system security requirements are met in the deployed system. This is to be accomplished by an independent third party approved by the Division Information Officer, Federal Finance, FMS. The report should contain a matrix tracing the requirements in the Security Plan and other requirements documents to the system component(s), including operational procedures, that satisfy the requirement.

Configuration Audit and Penetration Test Report. This report states the findings, potential impact, and recommended mitigations resulting from a thorough inside-out Configuration Audit and Penetration Test of the deployed system. This activity entails the systematic inspection, test, and analysis of the system's defensive mechanisms, networks, perimeter hosts, and key servers to assess that the system is suitably resistant to known vulnerabilities and attacks and properly implements established best security practices. This is to be accomplished by an independent third party approved by the Division Information Officer, Federal Finance, FMS.

4. Limited Official Use. All certification and accreditation documents shall be delivered marked "Limited Official Use Only" on front and rear covers, the spine of any binder used to deliver hard copy, and on top and bottom of each page.

5. Templates. Templates for all of the required certification and accreditation documents may be obtained from the Web addresses indicated or from FMS.

6. Roles. For purposes of the SSAA, the QLP shall be considered the "Program Manager" and the responsible FMS Division Director shall be considered the "Certifier." FMS shall be the system accreditor.

7. Independent Third Party. The QLP shall engage an independent third party to produce the Technical Vulnerability Assessment Report, the ST&E Report, and the Configuration Audit and Penetration Test Report, as well as to provide advice and assistance to FMS Certifier. The Division Information Officer, Federal Finance, FMS, must approve in advance the choice of an independent third party. FMS will compensate the QLP for the direct costs charged by the Independent Third Party.

8. C & A Process. Within 10 business days of being designated a financial agent for lockbox processing, the QLP shall meet with FMS to begin the Certification and Accreditation definition process. This definition process includes, but is not limited to, determining the certification level for the IT system. These levels include the following:

   Level 1: Basic security review requires completion of the system-relevant Security Activity Checklist. The system user or an independent certifier may complete the checklist.

   Level 2: Minimum analysis requires the completion of the system-relevant Security Activity Checklist and independent certification analysis.

   Level 3: Detail analysis requires the completion of the system-relevant Security Activity Checklist and a more in-depth, independent analysis.

   Level 4: Comprehensive analysis requires the completion of the system-relevant Security Activity Checklist and the most extensive independent analysis.

Reaccreditation. IT systems must be recertified and reaccredited at least every 3 years, or after a major enhancement or change that results in a significant modification of the operating environment or security controls.

IT Security Compliance Matrix. To the extent that IT systems are employed to support General Lockbox Services, the QLP shall submit for FMS' review and approval, prior to processing transactions, an IT Security Compliance Matrix, which shall include a listing of all policies and standards from FMS IT Security Policy and Standards Manuals, the extent to which the policies and standards apply to the QLP's IT systems, and the means of compliance with the policies and standards. The QLP shall certify the completeness and accuracy of the matrix.

Annual Responsibilities. Consistent with the provisions of FMS IT Security Policy and Standards Manuals, the QLP shall perform the following responsibilities at least annually, upon the anniversary of the most recently granted Authority to Operate:

1. Conduct a Security Review.
2. Update the Business Risk Assessment.
3. Certify that all user accounts/profiles/passwords and associated roles, and access control lists are current and appropriate.
4. Update the Security Activity Checklist or the Security Self-Assessment, as applicable.
5. Update the Security Plan (NIST 800-18).
6. Update the Technical Vulnerability Assessment Report.
7. Conduct IT security awareness training.
8. Update the IT Security Compliance Matrix.

9. Update Diagrams and Topologies and Component Lists.
10. Test continuity of operations and disaster recovery procedures.

Note that these annual reviews do not need to be completed during years when the IT system receives a full recertification and reaccreditation.

Quarterly Responsibilities. For IT systems certified at Levels 3 and 4, the QLP shall execute interim configuration audits and penetration tests quarterly, which shall include basic checks to ensure that no changes or new vulnerabilities have emerged since the last full configuration audit and penetration test, and checks for security-related patches and updates for all hardware, software, and networking components.

Security Officers. The QLP shall designate an information systems security officer (ISSO) responsible for the security of IT systems and compliance with IT policies and standards. The QLP shall ensure that any contractors that obtain or operate IT systems also designate an ISSO for these purposes. The QLP shall ensure that such designations are kept up to date. (See IEI Attachment K, ISSO Designation Template, available on FMS' Web site at www.fms.treas.gov/rebids/attachments.

Vendor Security Guidelines. To the maximum extent practicable, the QLP shall comply with all security instructions and documentation accompanying vendor hardware and software. The QLP shall thoroughly review all vendor recommendations and requirements for the configuration of security controls. If operational requirements dictate that such security recommendations cannot be met, the QLP shall document noncompliance prior to conducting any Technical Vulnerability Assessments or Configuration Audits and Penetration Tests.

Diagrams and Topologies. To the extent that IT systems are employed to support General Lockbox Services, the QLP shall provide a business process model diagram, a logical data flow diagram, and a physical and logical topology diagram.

Component Lists. To the extent that IT systems are employed to support General Lockbox Services, the QLP shall provide a list of all hardware, software, and networking equipment, including make, model, and release or version number.

Encryption Plan. To the extent that IT systems are employed to support General Lockbox Services, the QLP shall develop an encryption plan to be submitted to FMS for review and approval. The encryption plan shall include the following:

1. Identification of all telecommunications and sensitive data.
2. Encryption methods and algorithms.
3. Information on any commercial off-the-shelf products used, and compliance with NIST Federal Information Processing Standards Publication (FIPS PUB) 140 series.
4. Key management procedures for generation, distribution, storage, entry, use, and destruction.

4.12 Disaster Recovery And Processing Continuity Plans

Periodically, due to unexpected events or situations, normal day-to-day lockbox processing operations are interrupted, thereby resulting in less than 100% equipment/processing functionality. These unforeseen events can be attributed to but not limited to fire, earthquakes, floodwaters, storms, bombs, terrorist attacks, biochemical attacks, or hurricanes/tornadoes. Each QLP must develop an internal **Disaster Recovery and Processing Continuity Plans** for implementation in the event of such occurrence.

The Disaster Recovery and Processing Continuity Plans will outline the course of action QLPs will implement in the event an unexpected event occurs that prevents normal operation of the processing facility, which could be less than or more than 48 hours. QLPs are required to configure processing sites with an alternative power source, in the event of power failure, that will enable continuity of lockbox processing (at less than 100% equipment functionality) should a disaster or situation occur. Consequently, each QLP must have a designated contingency site established to accommodate daily lockbox processing in the event the primary processing facility is shutdown in excess of 48 hours. The plan should address assurance that all payments will be processed timely if an outage or other unforeseen event disrupts normal operations for less than 48 hours. Each processing site must have a Disaster Recovery Plan that addresses the following:

1. Workstation Processing,
2. Information Capture, Storage, and Retrieval,
3. Data Processing and Telecommunications,
4. Full Operations Emulation, and
5. Shut Down

At a minimum, the Disaster Recovery Plan must include:

1. If the site is unavailable for two or more days, Disaster Recovery Plans must include provisions for the work to be transferred to a contingency site. This plan must include maintaining a log recording the volumes, received dates, and new site location(s) for transferred work.
2. If the site is unavailable for a few hours or one day, the plan must stipulate that the work will be held at the QLP's site.
3. The Disaster Recovery Plan must include primary and secondary contact personnel for each processing site.

Disaster Recovery Plans must include specific arrangements coordinated with the post office in the event mail needs to be (1) transshipped to a contingency site in a disaster (e.g., mail will be forwarded by post office to another site/location); (2) mail will be packaged and picked up by a special lockbox courier; or (3) mail will be received as usual and prepared for transshipment by the QLP).

In addition, lockbox site disaster plans must include the stipulation that arrangements to send QLP production support personnel to the designated back-up facility will be made through a specific pre-arranged agreement with that site. Staff must cover expertise in all functional areas.

1. Document Extraction
2. Data Entry
3. Proof Operations
4. Manual/Exception Processing
5. Quality Review
6. Mail-Out/Packaging
7. Shipping

Disaster Recovery Plans must stipulate that if personnel are available, the mail will be sorted to identify high dollar amounts to be worked first regardless of mailing address or received dates. The back-up facility must agree to assume the responsibility for reporting into CA$HLINK II totals to FMS. The QLP agrees and understands that it shall remain liable for all delays in funds capability as provided under the DFA, Delay of Funds Availability, Section XII.

The plan must also stipulate that when the primary production facility is again available, multiple shifts and overtime will be utilized until the backlog situation is remedied.

All Disaster Recovery Plans must be tested at least once a year including system and application testing, where appropriate. An agreement by the QLP to provide annual testing schedules and results must be included in the plan. In addition, lockbox processing supervisors must agree to review disaster recovery procedures with all personnel twice each year. It will be the specific responsibility of the lockbox processing manager to review the disaster recovery plan with the Lockbox Management Team and update it as needed to ensure the test meets all of the business recovery needs.

APPENDIX 1

LEGAL AGREEMENTS – DFA and MOU

Designation and Authorization of {Name of Bank}
as Financial Agent
for General Lockbox Services

THIS DESIGNATION AND AUTHORIZATION OF FINANCIAL AGENT (DFA), dated as of _____, 2003 (Effective Date), is entered into by the Financial Management Service (FMS), a bureau of the United States Department of the Treasury (Treasury), as Principal, and {Insert FA Name} (Financial Agent), as a Depositary and Financial Agent of the United States. This DFA sets forth the terms and conditions required of the Financial Agent for the establishment and performance of general lockbox services.

Recitals

In furtherance of its role in managing collection and disbursement mechanisms of the United States, FMS designates qualified financial institutions as depositaries and financial agents to act on behalf of the United States to perform essential banking services. In consideration of those services, FMS may compensate its financial agents for performing such duties.

FMS has determined that it is in the interests of the United States to designate the Financial Agent to serve as a financial agent for the essential banking services described herein.

The Financial Agent, in accordance with the terms and conditions stated herein, desires to serve as financial agent for the United States.

Therefore, in consideration of the representations, warranties and mutual promises and agreements set forth herein, the Financial Agent and FMS agree as follows:

I. AUTHORITIES

The parties acknowledge and agree that:

A. The Secretary of the Treasury has authority to designate financial institutions as Depositaries and Financial Agents of the United States to perform essential banking services pursuant to 31 U.S.C. § 3303, 12 U.S.C. §§ 90 and 265 and other authorities. The Secretary of the Treasury has delegated to FMS the authority to select and designate depositaries and financial agents for, among other purposes, providing general lockbox services.

[6] As of the Effective Date of this DFA, the Draft Chapter 3000 of Volume V of the TFM, attached hereto as Attachment C is incorporated by reference. Once the draft is finalized and published, the final, published Chapter 3000 shall be deemed incorporated by reference herein.

B. This DFA is not a Federal procurement contract, and is therefore not subject to the provisions of the Federal Property and Administrative Service Act (40 U.S.C. § 471 et seq.), the Competition in Contracting Act (41 U.S.C. § 251-260) or the Federal Acquisition Regulations (48 CFR Chapter 1).

II. DESIGNATION AND AUTHORIZATION

Pursuant to 31 U.S.C. § 3303 and 12 U.S.C. §§ 90 and 265, and relying on the representations, warranties and promises contained herein, the Secretary of the Treasury, through FMS, hereby designates and authorizes the Financial Agent to act as depositary and financial agent for general lockbox services, subject to the terms and conditions of this DFA, which set forth the scope of the agency. The scope of the Financial Agent's authority will be further defined in memoranda of understanding entered into by and among the Financial Agent, FMS and Federal agencies requiring lockbox services. (The term "MOU," as used herein, refers to such three-party agreements for performance of services pursuant to this DFA.) Additionally, FMS may, from time to time, issue instructional bulletins, consistent with this DFA, which further describe the scope of authority and financial agent responsibilities under this DFA. This DFA does not guarantee that the Financial Agent will be awarded any work pursuant to an MOU. The Financial Agent acknowledges that it will not be authorized to perform services until such an MOU becomes effective.

III. INCORPORATION BY REFERENCE

The following, as from time to time amended, are incorporated herein by reference and given the same force and effect as though fully set forth herein:

- 31 CFR Part 202;
- Invitation for Expressions of Interest (IEI), Section 4.0, "Technical Requirements", including all amendments and modifications thereto (collectively referred to as the "Technical Requirements") (See Attachment A);
- The Pricing Schedule (See Attachment B);
- The Financial Agent's Response to the IEI, including its Certification Statement (See Attachment C);
- Volume V, Chapter 3000 of the Treasury Financial Manual (TFM) (V TFM Chapter 3000)[7] (See Attachment D);
- V TFM Chapter 2000, Supplement 1, governing CA$HLINK Bank Management Reporting;
- V TFM Chapter 2000, Supplement 2, CA$HLINK User's Guide;
- I TFM part 5, Chapter 4600.

[7] As of the Effective Date of this DFA, the Draft Chapter 3000 of Volume V of the TFM, attached hereto as Attachment D is incorporated by reference. Once the draft is finalized and published, the final, published Chapter 3000 shall be deemed incorporated by reference herein.

In the event of inconsistencies between this DFA, including any addenda or amendments hereto, and any documents incorporated by reference, the provisions of this DFA shall govern, to the extent it is consistent with Federal law.

IV. REPRESENTATIONS AND WARRANTIES

The Financial Agent hereby represents and warrants to FMS the following (which shall survive the execution and delivery of this DFA, the truth and accuracy of which are a continuing condition of FMS' obligations under this DFA):

A. The Financial Agent meets the class and eligibility requirements of a Depositary and Financial Agent of the Government as stated in 31 CFR Part 202.

B. The Financial Agent is not aware of any legal or financial impediments to performing its fiduciary responsibilities and obligations under this DFA, which it has not disclosed in writing to FMS.

C. Neither the Financial Agent, nor, to the best of the Financial Agent's knowledge, its contractors or representatives have offered or given a bribe or gratuity (including but not limited to entertainment and gifts) to an officer, official or employee of Treasury.

D. The Financial Agent has full corporate power and authority to enter into and execute and deliver this DFA and to carry out and perform its obligations hereunder.

E. This Financial Agent has duly and properly executed this DFA.

F. All information contained in any document the Financial Agent signed as part of the bid process for services performed pursuant to this DFA remain true and accurate, unless otherwise disclosed in writing to FMS.

V. SERVICES TO BE PERFORMED BY AGENT

A. Compliance with the Technical Requirements. The Financial Agent shall comply with all requirements, terms and conditions set forth for Qualified Lockbox Providers (QLPs) in the Technical Requirements and in any MOU. The Financial Agent acknowledges that the performance of obligations in the Technical Requirements and any MOUs is vital to the United States Treasury and the people of the United States.

B. 31 CFR Part 210. To Financial Agent warrants that it shall comply at all times with the provisions of 31 CFR Part 210, to the extent they are applicable to work performed pursuant to this DFA.

C. Fiduciary Responsibility. With respect to carrying out its fiduciary responsibilities under this DFA, the Financial Agent agrees to act at all times in the best interests of the United States. FMS may from time to time issue guidance, consistent with the terms of the DFA, regarding the Financial Agent's fiduciary responsibilities. The Financial Agent agrees to comply with this guidance to the same extent it complies with the terms of this DFA.

D. Financial Agent Contracts. The Financial Agent will use its own employees to carry out its obligations hereunder, except that the Financial Agent may hire other financial institutions or third parties as contractors to fulfill its obligations hereunder only in accordance with the requirements and limitations of the Technical Requirements Section 4.8. "Contractors". All work shall be performed under the supervision and control of the Financial Agent and its responsible employees. Contractors who are not designated as depositaries and financial agents under 31 CFR Part 202 shall not control or possess public funds at any time.

E. Status of Financial Agent Contractors. Any contractors hired by the Financial Agent for purposes of carrying out its obligations hereunder, shall not be contractors, subcontractors, or subagents of FMS. FMS shall not be deemed a party to any contract that the Financial Agent enters into with a third party (other than an MOU) in order to fulfill its obligations hereunder. FMS shall not be liable for any compensation due to any contractors used by the Financial Agent.

F. Information, Personnel and Physical Security. The Financial Agent shall ensure that the required level of information, personnel and physical security is provided and maintained in accordance with the requirements set forth in Section 4.10 and 4.11 of the IEI, "Security Requirements", and all other documents incorporated by reference herein. In particular, the Financial Agent shall comply with the Computer Security Act of 1987 (Public Law 100-235) and all applicable standards and regulations established thereunder, as directed by FMS. Additionally, the Financial Agent shall not publish or disclose in any manner, without FMS' written consent, the details of any safeguards either designed or developed by the Financial Agent pursuant to this DFA or otherwise provided by FMS or other Federal agency. FMS must notify the Financial Agent in writing that it has met all security requirements prior to entering into an MOU or receiving any compensation hereunder. FMS may amend such requirements from time to time as necessary to protect the security, confidentiality and integrity of the Treasury's collection systems and data and to maintain compliance with all applicable laws and policies affecting lockbox collections.

G. Privacy Act.

1. The Financial Agent may be required to design, develop, operate or maintain a system of records on individuals or businesses to accomplish a government-required function that is subject to the Privacy Act of 1974 (5 U.S.C. § 552a), as amended (hereinafter, "the Act") and applicable Treasury regulations. Violations of the Act may involve the imposition of criminal penalties. Any information subject to the Act made available to the Financial Agent (or any contractor performing services for the Financial Agent in connection with this DFA) shall only be used for the purpose of carrying out the provisions of this DFA and any MOU, and shall not otherwise be divulged or made known in any manner to any person except as may be required by law.

2. The Financial Agent shall inform its officers and employees (and any contractor officers and employees) to whom information is or may be disclosed of the penalties imposed under the Act for improper disclosure of information. For example, 5 U.S.C. § 552a(i)(1), which

is made applicable to the Financial Agent by 5 U.S.C. § 552a(m), provides that any officer or employee of the financial institution who, by his /her employment or official position, has possession of, or access to, agency records, the disclosure of which is prohibited by the Act or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more that $5,000.

3. The Financial Agent shall train all officers and employees (and any contractor officers and employees) on the duties and responsibilities imposed on them and the rights conferred on individuals by the Act and Treasury regulations. The Financial Agent shall certify, in writing, that all employees and contractor employees (or any future employees) have received this training before they begin any tasks under which they may gain access to any information subject to the Act. A certification form for all training provided in support of this task order shall be signed by each Financial Agent employee and contractor employee and maintained on file by the Financial Agent. The Financial Agent shall make these certifications available for reasonable review by FMS (or other Treasury Department) personnel. The Financial Agent shall ensure that information concerning the Act's requirements is posted in appropriate places (including computer systems/databases) to continually remind employees and contractor employees of their responsibilities under the Act.

H. Right to Examine and Audit. FMS, the Treasury Inspector General's Office, and the General Accounting Office shall have the right to conduct announced or unannounced, on-site security reviews and audits of the Financial Agent's (and any contractor's) facilities, operations, books and records related to the Financial Agent's performance hereunder. Federal agencies for which the Financial Agent is performing lockbox services shall also have the right to conduct such reviews and audits.

I. Access to Systems. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of data, the Financial Agent shall afford FMS, its agents and contractors access to the Financial Agent's facilities, installations, technical capabilities, operations, documentation, records, and databases. If new or unanticipated threats or hazards are discovered by either FMS or the Financial Agent, or if existing safeguards have ceased to function, the party discovering such problem shall immediately bring the situation to the attention of the other party. If the Financial Agent requests that any FMS contractor assisting FMS in the performance of an inspection sign a confidentiality agreement, FMS shall require the contractor to sign the confidentiality agreement attached as Attachment E hereto. The Financial Agent shall afford the contractor access if such confidentiality agreement is signed.

J. Continuity of Services. The Financial Agent recognizes that the services provided under this DFA are vital to the U.S. Treasury and must be continued without interruption, and that, upon the expiration or termination of this DFA, FMS may designate another financial institution to provide the services required hereunder. Upon expiration of this DFA, the Financial Agent shall, unless otherwise directed in writing by FMS, provide all transition

services specified in Section 4.9.4 of the Technical Requirements.

K. Marketing. The Financial Agent understands and acknowledges that it is designated for the purpose of providing lockbox services only. This DFA does not designate or authorize the Financial Agent to provide any other depositary, cash management, or financial management service. The Financial Agent shall not market any other financial services to Federal agencies without the prior written consent of FMS to expand the scope of designation.

L. Records Retention. The Financial Institution shall retain all records in accordance with section 4.9.5 of the Technical Requirements.

VI. COMPLIANCE WITH APPLICABLE LAWS

The Financial Agent shall, at all times, be in compliance with all Federal, State and local laws applicable to its performance under this DFA.

VII. PRICING AND COMPENSATION

A. Method of Compensation. FMS will compensate the Financial Agent for services provided under this DFA in such method or methods as FMS deems appropriate in its sole discretion. The methods of compensation include, but are not limited to, compensating balances, direct payment, and Depositary Compensation Securities as offered and described in 31 CFR Part 348, or any other method upon which FMS and the Financial Agent mutually agree.

B. Pricing. The amount of compensation for all charges shall be determined in accordance with the Pricing Schedule attached hereto as Attachment B.

C. Option Period Pricing. The prices for required services provided during any Option Period are governed by the terms set forth in Attachment B.

D. Compensation for Transition Services. The Financial Agent will be compensated for all transition services in accordance with Section 4.9.4 of the Technical Requirements.

E. Compensation After Termination. If this DFA is terminated pursuant to Articles XI or XVII, the Financial Agent shall be compensated only for services received and accepted by FMS prior to the effective date of termination. The Financial Agent shall not be compensated for lost profits or business opportunities the Financial Agent would have expected after the expiration of the term in which this DFA is terminated.

F. FMS Execution of MOU Required For Compensation. FMS must be a party to any and all MOUs entered into pursuant to this DFA. The Financial Agent will not be compensated for any services performed pursuant to any agreement to which FMS is not a party.

VIII. TRANSFER OF AGREEMENT

A. Transfer or Assignment Prohibited. The transfer or assignment of this DFA by sale, operation of law, or other means, is prohibited and shall be considered a Default pursuant to Article X, paragraph A, unless the conditions of the following paragraph B are met.

B. Surviving Entity in a Merger or Acquisition. The transfer shall not be considered a Default if:

1. The successor financial institution's (SFI) interest arises out of the transfer of all the Financial Agent's assets or the entire portion of the assets involved in performing this DFA. (Examples include, but are not limited to, sales of these assets with a provision for assuming and transfer of these assets incident to a merger or corporate consolidation);

2. The SFI meets the class and eligibility requirements of a Depositary and Financial Agent under 31 CFR Part 202; and

3. The conditions of Article IX "Mergers and Consolidation" are met.

C. Written Acceptance Required. No SFI shall be considered acceptable to FMS to act as the Financial Agent under this DFA unless FMS expressly sets forth its acceptance in writing to the SFI. Notwithstanding paragraph B above, if FMS, in its sole discretion, determines that it is not in the best interests of the United States to accept the SFI, then FMS may terminate this DFA, pursuant to Article XVII herein.

D. SFI Bound by DFA. If FMS allows assignment of this DFA to the SFI, the SFI shall assume all obligations, liabilities and responsibilities and meet all conditions required of the Financial institution under this DFA and shall continue operations and performance without interruption, unless otherwise directed in writing by FMS. In the event of a default under this Article X, the SFI shall remain obligated to perform pursuant to this DFA, unless FMS sends written notice that it intends to terminate this DFA pursuant to Article XI.

E. Cooperation of SFI. If the SFI is not acceptable to FMS, the Financial Agent (or the SFI, as applicable) agrees to cooperate and act in good faith in assisting FMS to ensure the smooth transition of lockbox processing to the selected Financial Agent. All terms and conditions identified under Article V, paragraph J, "Continuity of Services," shall apply.

IX. MERGER AND CONSOLIDATION

A. Prior Written Notice to FMS. The Financial Agent shall give written notice to FMS prior to the sale of the assets involved in the performance of this DFA or the merger or consolidation of the Financial Agent with another entity. Notice shall be delivered simultaneously with notice to Federal banking regulators and prior to such action becoming public knowledge, consistent with Federal laws and regulations. FMS agrees to keep all such information confidential.

B. Documents Relating to the Transaction. In the case of a merger or consolidation involving the Financial Agent, promptly upon FMS' request, the Financial Agent, or its SFI, shall furnish, or cause to be furnished to FMS, true, correct and complete copies of all agreements, documents and instruments relating to such merger or consolidation, including, but not limited to, the certificate or certificates of merger or consolidation as filed with each appropriate Secretary of State and any documents required to be filed with any State or Federal regulatory agencies having authority over the Financial Agent's operations.

C. Documents of Surviving Entity. FMS shall have the right to examine documents of the surviving entity that FMS deems germane to this DFA to determine whether FMS finds it to be an acceptable successor under this DFA.

D. Confirmation of Obligations. The SFI shall, immediately upon the effectiveness of the merger or consolidation, expressly confirm in writing, its obligation to perform hereunder.

X. DEFAULTS

The following constitute defaults under this DFA:

A. Non-performance. The Financial Agent fails to duly perform or comply with any of the obligations or conditions contained in this DFA (including, but not limited to, any and all terms incorporated by reference herein or any MOU), and, if applicable, such failure continues beyond any time period granted to cure such failure.

B. Loss to U.S. Treasury. Any negligent, willful or reckless act of the Financial Agent or its contractors that results in a loss to the U.S. Treasury.

C. Breach of Fiduciary Duty. The Financial Agent breaches its fiduciary duty to the United States with respect to its agent responsibilities.

D. Misrepresentation. Any representation made herein or provided to FMS pursuant to the IEI was materially false, incorrect, or incomplete when made.

E. Insolvency. The Financial Agent becomes insolvent or generally fails to pay, or admits its inability to pay, debts as they become due or makes a general assignment for the benefit of any of its creditors.

F. Bankruptcy Proceedings. Any bankruptcy, reorganization, liquidation, dissolution or other case and proceeding under any bankruptcy or insolvency law is commenced in respect of the Financial Agent.

G. Appointment of Receiver. A receiver, trustee, conservator or other custodian is appointed for any of the property of the Financial Agent.

XI. REMEDIES FOR DEFAULT

A. FMS Actions. FMS may take any or all of the following actions in the event of a default, as described in Article X "Defaults" above:

1. Terminate This DFA. FMS may revoke, in whole or in part, this DFA and cease its performance hereunder. If this DFA is terminated, the designation and authorization of the Financial Agent as financial agent for purposes of general lockbox services under this DFA is automatically revoked. If FMS terminates this DFA, the Financial Agent shall cease all operations hereunder (including all services performed pursuant to any MOUs) as of the effective date of termination stated in the notification of termination. The Financial Agent shall remain obligated to comply with Article V, paragraph J, "Continuity of Services" herein.

2. Terminate an MOU. FMS may terminate one or more MOUs, which FMS, in its sole discretion, determines should be terminated, based upon the nature of the Financial Agent's default.

3. Revoke Financial Agent Status. FMS may revoke the Financial Agent's designation as a depositary and financial agent for the United States pursuant to 31 CFR Part 202. This DFA and any other agreement with the Treasury requiring status as a depositary and financial agent shall be deemed terminated as of the effective date of such revocation.

4. Probation. FMS may place the Financial Agent in probationary status while assessing the desirability of allowing the Financial Agent to continue to perform essential banking services for FMS under this DFA or any other agreement with FMS. During such probationary time, the Financial Agent may not bid on additional FMS services.

5. Future Work as Financial Agent. FMS may factor information regarding any default hereunder when making any decisions regarding future use of the Financial Agent for performance of financial agent services, including, but not limited to, using such information in the award of work pursuant to an invitation for expressions of interest or other bid process.

6. Liquidate Collateral. FMS may liquidate collateral pledged pursuant to 31 CFR 202.6.

7. Determine Method of Compensation. If any default should cause a loss to the United States Treasury, FMS may, in its sole discretion, determine the means of compensating the Treasury for such loss in accordance with Article XII, paragraph E herein.

B. Optional Notice and Opportunity to Cure. Prior to taking action under this Article XI, FMS may, but is not obligated to, give the Financial Agent up to 30 calendar days from the date of notification to propose, in writing, a plan and timetable to resolve any deficiencies. The Financial Agent expressly acknowledges that FMS is under no obligation in any case to give the Financial Agent an opportunity to resolve the deficiencies before taking action under this Article XI. To the extent that FMS, in its sole discretion, does give the Financial Agent the opportunity

to propose a plan and timetable to resolve the deficiencies, the sufficiency of such plan and timetable will be determined by FMS, in its sole discretion. If FMS makes the determination that the proposed plan and timetable to resolve the deficiencies are insufficient, FMS may take any action under this Article XI that FMS deems necessary or advisable.

C. Financial Agent's Obligations When DFA is Revoked. When the Financial Agent's status as a depositary and financial agent for DFA services is revoked, it shall provide transition services as required and specified under Article V, paragraph J, "Continuity of Services," herein.

XII. FINANCIAL INSTITUTION LIABILITY

A. Liability. The Financial Agent shall fully reimburse the Government for any public funds lost as a result of a breach of this DFA. In addition, the Financial Agent shall reimburse the Government for its costs and expenses associated with any such breach. The method of determining and recovering these costs will be at the sole discretion of FMS. The Financial Agent expressly assumes liability for the negligence, recklessness, and/or willful misconduct of its officers, employees, agents, contractors and temporary employees. In the event that a third party brings a claim against the Financial Agent for actions it has taken contrary to, or outside the scope of, this DFA, the Financial Agent may not bring a claim, in any form or at any time, against Treasury, its employees, or officers for the cost or liabilities incurred by the Financial Agent defending or paying any such claim.

B. Delay of Funds Availability. If any act on the part of the Financial Agent (including its contractors) results in a delay of funds availability, or other loss to the U.S. Treasury, the Financial Agent shall fully reimburse the U.S. Treasury for the amount of such loss. The liability for delays in funds availability equals the time "Value of Funds" as more fully described in Volume V of the Treasury Financial Manual. Notwithstanding the foregoing, the Financial Agent will not be liable for the time Value of Funds on the amount delayed or any excess costs if: (a) the funds transfer delay or failure to perform arises out of acts of God (e.g. fires, floods, epidemics, quarantine restrictions, and unusually severe weather), the public enemy, the U.S. Government in either its sovereign or contractual capacity, or strikes or freight embargoes; (b) the Financial Agent (or any of its contractors) did not have use of the funds delayed or did not realize unjust enrichment; and (c) the Financial Agent (or its contractors) could not have prevented the delay of funds availability, or other loss to the U.S. Treasury, by obtaining required services from other sources in sufficient time to prevent or avoid such delay or loss.

C. Costs Incurred for Obtaining Other Services. Revocation of the Financial Agent's status as a depositary and financial agent pursuant to the Financial Agent's default under this DFA may require FMS to obtain other services similar to those required under this DFA. The Financial Agent shall be liable to FMS for its reasonable costs incurred obtaining such substitute services.

D. Method of Collecting Reimbursement. After the formal Disputes process set forth in section 4.9.3 of the Technical Requirements has been completed, FMS will, in its sole discretion, determine the method to make the party who lost value whole. The preferred method of

collection is by means of an adjustment to the Financial Agent's compensating balance Treasury Time Balance (TTB) account cumulative position. However, FMS has the discretion to collect any monies due to FMS from the Financial Agent by means of a direct payment to the Treasury's General Account at an FRB. The methods of direct payment from the Financial Agent include, but are not limited to, an ACH debit, receipt of a hard dollar payment, a charge against the Financial Agent's reserve account at the FRB, and a liquidation of collateral pledged to secure deposits of public money. In the event that FMS directly bills the Financial Agent, the Financial Agent shall remit the amount set forth in the Value of Funds Assessment decision. If the Financial Agent fails to pay such amount within the time specified, the Financial Agent shall be held liable for interest, penalties, and administrative costs in accordance with the authorities codified at 31 U.S.C. § 3717 and 31 CFR Parts 5 and 900-904.

XIII. REPAYMENT OF EXCESS FUNDS TRANSFERRED TO TREASURY

In the event excess funds are transferred from the Financial Agent, FMS will be liable to the Financial Agent for the time Value of Funds of the excess so transferred, less any expenses incurred by FMS. FMS will not charge expenses if the transfer was directed by FMS.

XIV. NO WAIVER

Failure on the part of FMS to insist upon strict compliance with any of the terms, covenants and conditions hereof shall not be deemed a waiver of such terms, covenants and conditions, nor shall any waiver or relinquishment of any right or power hereunder at any one or more times be deemed a waiver or relinquishment of such right or power at any other time or times. No waiver shall be valid unless in writing and signed by an authorized officer of FMS. No failure to exercise and no delay in exercising, on the part of FMS, any right, remedy, power or privilege, hereunder, shall operate as a waiver thereof; nor shall any single or partial exercise of any right, remedy, power or privilege hereunder preclude any other or further exercise thereof or the exercise of any other right, remedy, power or privilege. The rights, remedies, powers and privileges herein provided are cumulative and not exhaustive of any rights, remedies, powers and privileges provided by law.

XV. RIGHTS TO SOFTWARE, DATA AND RECORDS

A. Rights to Program Software and Business Methods. FMS shall have non-exclusive unlimited rights in the ideas, concepts, design, and business methods developed for performance of lockbox services pursuant to this DFA. "Unlimited rights" means the right of FMS to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so. Immediately upon termination or expiration of this DFA, the Financial Agent shall provide the databases, output formats and software used in the performance of its obligations hereunder. Notwithstanding any provisions to the contrary contained in any standard commercial license or lease agreement, FMS shall have limited rights to any restricted computer software that is necessary to operate any general lockbox services pursuant to this DFA. "Restricted computer software" means any computer program, computer database, or

documentation thereof, that has been developed at private expense and either is a trade secret, is commercial or financial and confidential or privileged, or is published and copyrighted. If the restricted computer software delivered under this DFA is published and copyrighted, it is licensed to the Government, without disclosure prohibitions. "Limited rights" means that FMS may: (a) use, or copy the software for use in or with the computer or computers accessing the data or services provided under this DFA; (b) reproduce the software for safekeeping or backup purposes; (c) modify, adapt, or combine the software with other computer software, provided that the modified, combined, or adapted portions of the derivative software are made subject to the same limited rights.

B. Rights to Data and Records. Any records (including, but not limited to, working papers and design documents) and data supplied to the Financial Agent by FMS, or collected by the Financial Agent in performance of this DFA, shall remain the exclusive property of FMS. The Financial Agent shall not use, copy, or distribute such data or records in any manner except as necessary for carrying out its responsibilities under this DFA. Such data includes, but is not limited to, names, addresses and other information about individuals and businesses making payments to, or receiving payments from, the U.S. Treasury and software which FMS supplies to the Financial Agent in connection with this DFA. (See Article V, paragraph G of this DFA regarding Privacy Act requirements.

XVI. DISPUTES

A. General. The parties agree that it is in their mutual interest to resolve disputes by agreement. If a dispute arises from the implementation or administration of this DFA, the parties will make all reasonable efforts to resolve the dispute by mutual agreement.

B. Formal Dispute. If the dispute cannot be resolved informally by mutual agreement, the dispute shall be resolved pursuant to Technical Requirements section 4.9.3. The Financial Agent shall exhaust this administrative remedy prior to commencing legal proceedings.

C. Obligation to Continue Performance. The Financial Agent shall proceed diligently with performance of the services required by the DFA pending final resolution of any dispute.

D. Other Remedies. FMS and the Financial Agent have the right to pursue any and all available legal or equitable rights they may have notwithstanding any written decision that results from the formal dispute process.

XVII. BEST INTERESTS OF THE UNITED STATES.

A. FMS Actions. The Financial Agent acknowledges that the United States must have complete control of public monies at all times. Therefore, notwithstanding any other provisions of this DFA, when FMS, in its sole discretion, determines such actions are necessary to protect the interests of the United States, FMS may take the following actions even in the absence of any of the conditions set forth in Article X "Defaults":

1. Terminate this DFA with 30 days written notice.
2. Revoke the Financial Agent's status as a depositary and financial agent.
3. Recall immediately any compensating balances placed with the financial institution.
4. Call immediately any deposit securities prior to their stated maturity.

If practicable, FMS will give the Financial Agent up to fourteen (14) calendar days notice before recalling the compensating balances and deposit securities referenced in clauses 3 and 4 above; however, FMS reserves the right in all cases to recall such balances and securities immediately by providing only one (1) calendar day notice to the Financial Agent.

B. Transition. If FMS terminates the DFA pursuant to this Article XVII, FMS may designate another financial institution to provide the services required hereunder. In such instance, the Financial Agent shall, unless otherwise directed in writing by FMS, provide the all transition services specified in the Technical Requirements.

XVIII. MODIFICATIONS

A. FMS' Right to Modify. FMS may, in its sole discretion, modify, add to, or amend the general scope of, and terms and conditions for providing, required services under this DFA, including incorporated documents and requirements, by providing written notice to the Financial Agent.

B. Adjustment to Compensation. If any such modification, addition, or amendment causes an increase or decrease in the cost of, or the time required for, performance of any service required by this DFA, FMS will make an equitable adjustment in the service price or other terms of performance, or both, and this DFA and any applicable MOU shall be modified accordingly. If the Financial Agent realizes a savings in the cost of required services as a result of the new procedures, operations, or changes such savings shall be reflected in a downward adjustment to the DFA Price Schedule.

C. Financial Agent Duty to Notify.

1. Change in Cost of Services. If the Financial Agent regards any communication from FMS to be a modification of the services required under this DFA, the Financial Agent shall notify FMS, in writing, within 30 calendar days from the date that the Financial Agent receives such communication. The Financial Agent must notify FMS if it realizes a cost savings. Notwithstanding the preceding paragraph B, FMS will bear no obligation to compensate the Financial Agent for any additional costs, unless such notice is timely received. If the parties fail to agree to any adjustment in price, FMS shall treat the request for a price adjustment as a dispute, and it will be settled in accordance with section 4.9.3 of the Technical Requirements.

2. Software or Hardware Modifications. If any modification, addition, or amendment, or other change requires software or hardware modification, the Financial Agent shall provide FMS with written notification at least 30 calendar days prior to the Financial Agent

authorizing any work. If FMS approves of the modification work, in writing, the Financial Agent shall place an order for programming or equipment with the vendor of its choice within 30 calendar days of FMS' notice of approval.

XIX. PROVISION OF DATA

Prior to the expiration of this DFA, FMS may solicit financial institutions to function as depositaries and financial agent for general lockbox services. The Financial Agent shall provide essential activity data and other information upon request. The Financial Agent may be required to provide data to an independent firm to conduct a nationwide mail study. The Financial Agent shall fully cooperate in all data-gathering activities at no cost to FMS.

XX. INITIAL TERM OF FINANCIAL AGENT AGREEMENT

This DFA shall become effective as of the Effective Date, and shall remain in effect for three (3) years (Initial Term), unless earlier terminated pursuant to Articles XI, "Remedies for Default," or XVII, "Best Interests of the United States," herein.

XXI. FMS OPTIONS TO RENEW

A. FMS Options. FMS, in its sole discretion, shall have two (2) successive options to renew this DFA for a period of two (2) years each (Renewal Periods), which FMS shall exercise by giving written notice at least thirty (30) calendar days prior to the expiration of the Initial Term or the applicable Renewal Period. In the event FMS chooses to exercise an option to renew, all requirements, terms and conditions identified in this DFA and incorporated documents shall be effective for the Renewal Period, unless otherwise modified by FMS. The pricing of services for any renewal period are set forth in Attachment B hereto.

B. Extension Beyond Renewal Periods. Notwithstanding any provision herein to the contrary, FMS shall have the right to extend the term of this DFA beyond the expiration date of the last Renewal Period, if FMS determines that it is in the best interests of the United States to do so. FMS shall exercise this right by giving the Financial Agent written notice at least 60 calendar days prior to the expiration of the current term of this DFA. In the event this right of extension is exercised by FMS, all requirements, terms and conditions identified in this DFA, including incorporated documents and requirements, shall be effective for the term of the extension, unless otherwise modified by FMS. The pricing of services for the extension period shall be as set forth in Attachment B hereto.

C. Pricing Disputes. Any failure to reach an agreement on a proposed price adjustment shall be resolved pursuant to the Disputes process set forth in Section 4.9.3 of the Technical Requirements.

XXII. NOTICES

All notices required to be given herein shall be given to the following contacts unless expressly stated otherwise herein:

To FMS (other than the ATO):
Director, Financial Services Division
Financial Management Service
401 14th Street, SW
Washington, DC 20227

To the FMS ATO:
Director, Cash Management Directorate
Financial Management Service
401 14th Street, SW
Washington, DC 20227

To the Financial Agent:
[Contact Title/Office Information]

XXIII. MISCELLANEOUS

A. Counterparts. This DFA may be executed in two or more counterparts (and by different parties on separate counterparts), each of which shall be an original, but all of which together shall constitute one and the same instrument.

B. Third-Party Beneficiaries. This DFA will inure to the benefit of and be binding upon the parties hereto. No other person will have any right or obligation hereunder, except for Successor Financial Agents as described in Article VIII herein.

C. Headings. The headings herein are for purposes of reference only and shall not otherwise affect the meaning or interpretation of any provision hereof.

D. Officials Not to Benefit. No member of, or delegate to, Congress, or resident commissioner, or other U.S. Government official, shall be permitted to share in any part of this DFA, or to receive any benefit arising from it.

E. Gratuities. The Financial Agent, its contractors or representatives shall not offer or give a gratuity (including but not limited to entertainment and gifts) to an officer, official or employee of FMS or other bureau or unit of the Treasury Department.

F. Federal Law Applies. The parties agree that this DFA agreement will be interpreted under Federal law, but not under the Federal Acquisition Regulation, since it is not a procurement subject to the Federal Property and Administrative Service Act (41 U.S.C. §§ 251-260). In the absence of applicable Federal law, this DFA shall be interpreted pursuant to the laws

of the State of New York, without regard to its principles of conflict of laws

G. FMS Not Liable for Acts Exceeding the Scope of Authority. FMS will not be liable for any actions taken by the Financial Agent, which are outside of the scope of authority contained in this DFA.

H. Binding Effect of Agreement. This DFA shall be binding upon the Financial Agent and its successors and assigns.

XXIV. DEFINITIONS

Terms that are not defined herein are defined in Volume V, Chapter 3000, of the TFM.

Acceptance of Terms and Commitment

The signing of this document by authorized officials forms a binding commitment between FMS and the designated Financial Agent. The parties are obligated to perform in accordance with the terms and conditions of this document, any properly executed modification, addition, or amendment thereto, any Attachment thereto, and any documents and requirements incorporated by reference.

By their signing, the signatories represent and certify that they possess the authority to bind their respective organizations to the terms of this document, and hereby do so.

IN WITNESS WHEREOF, the Financial Agent and FMS by the following officials sign their names to enter into this DFA.

_____	_____
Date	_____, Director, Financial Services Division
_____	_____
Date	Financial Agent Authorized Bank Official/Title

Attachments:

Attachment A: Invitation for Expressions of Interest (IEI), Section 4.0, "Technical Requirements", including all amendments and modifications thereto

Attachment B: Pricing Schedule

Attachment C: The Financial Agent’s Response to the IEI, including its Certification Statement

Attachment D: Draft Volume V, Chapter 3000 of the Treasury Financial Manual

Attachment E: FMS Form Confidentiality Agreement

Memorandum of Understanding
Establishing General Lockbox Processing Guidelines for
{Insert Name of Payment Stream}

This Memorandum of Understanding (this "MOU") is entered into by and among, the U.S. Department of Treasury's Financial Management Service ("FMS"), the { Insert name of Financial Institution} ("Financial Institution"), and {insert name of Federal Agency requiring lockbox services} ("Agency"), in order to establish a lockbox service arrangement pursuant to the Designation and Authorization of {Insert name of Financial Institution} as Financial Agent for General Lockbox Services, entered into by and between FMS, as principal, and the Financial Institution, as agent, dated {insert effective date of DFA} ("DFA").

In accordance with Article II of the DFA, this MOU establishes roles and responsibilities of the parties with respect to processing {insert name of payment stream}. The specific lockbox requirements for this MOU are contained in the attached Statement of Work (SOW), which is incorporated by reference herein.

The term of this MOU is concurrent with the term of the DFA. Thus, this MOU expires when the DFA expires. Any dispute arising under this MOU will be addressed and resolved in accordance with the DFA Disputes Clause (DFA, Article XVI).

By their signing, the officials below represent and certify that they possess the authority to bind their respective organizations to the terms of this MOU, and hereby do so.

FINANCIAL MANAGEMENT SERVICE

By: _____ _____
Name: Date
Title:

{NAME OF FINANCIAL INSTITUTION}

By: _____ _____
Name: Date
Title:

{NAME OF FEDERAL AGENCY}

By: _____ _____
Name: Date
Title:

APPENDIX 2

TECHNICAL EVALUATION CRITERIA

GENERAL LOCKBOX NETWORK
TECHNICAL EVALUATION CRITERIA

CATEGORY	CRITERIA	MAXIMUM POINTS - 45
STAFFING/ PERSONNEL	1. Process for ensuring the coordination and communication between the account relationship officer, the lockbox operations staff, and the customer service department. 2. Staffing strategy for peak periods and for avoiding holdovers. 3. Procedures for back-up personnel and cross training within a function. 4. Quality improvement program, including performance measurement reports for monitoring quality/performance and address incentive programs. 5. Preparation and mailing of account analysis or billing statements to clients. 6. Forwarding of bank management or billing information to clients via EDI 822 (Customer Account Analysis Transaction Set). 7. Ability to meet all the reporting requirements for bank management according to the Treasury Financial Manual (TFM) Volume V, Part 1, Chapter 3000, Section 3060.	Staffing and Management Personnel combined, equals a total of 45 points.
MANAGEMENT PERSONNEL	1. Ability of key management personnel on-site at each lockbox location site. Coordination, responsibility, and communication with FI employees and contractors. 2. Support senior management provides in the search for improvement maintaining quality control and encouraging innovative solutions for these services. 3. Approach to account administration, e.g., account team, client account executives, support by administrative units, etc. Support staff in terms of size and hours of availability. 4. Organization charts showing lines of authority, resumes of the Principal Manager, Operations Manager, and other key contacts responsible for this effort.	

CATEGORY	CRITERIA	MAXIMUM POINTS - 55
MAIL PROCESSING/ HANDLING	1. The financial institution's schedule for post office pickups of mail for weekdays, weekends, and holidays. 2. The distance to the post office, the average length of time between the pickup of items at the post office and delivery to lockbox department. Information on who picks up the items from the post office (courier or internally managed) and who manages this arrangement. 3. Maintenance of a unique five-digit Zip code assigned exclusively for receipt of wholesale and retail lockbox items. If not applicable, the impact on mail delivery and sorting for lockbox processing. 4. Security procedures for mail delivered to the lockbox processing site from the post office. 5. The mail-sorting operation. Includes manual and automated handling, ability to read bar codes, peak volume, and contingency plans. The receipt and handling of remittances delivered by private services (e.g., Federal Express, UPS, and/or courier) to the lockbox for processing. 6. Procedures to expedite the sorting of mail for high-dollar boxes. 7. Procedures for the control and processing of cash received in remittance envelopes including dual controls, if any. 8. Methods for monitoring mail deliveries so that any U.S. Postal Service changes affecting those deliveries and processing are identified as early as possible. 9. The process for implementing customer-specific changes, or changes that may be necessary due to a high-volume customer that is added to volume mix and originates from several different regions.	

CATEGORY	CRITERIA	MAXIMUM POINTS - 60
DATA CAPTURE/ TRANSMISSION	1. Procedures for the capture and transmission of remittance detail, such as account or invoice number or other data for automated posting of accounts receivable records. 2. Procedures for retaining the actual check in the lockbox department until data capture is completed or sending them to the financial institution for collection prior to data capture. 3. Process for work requiring data capture (through input by keypunch operators) is processed. 4. Types of image technology used such as the Courtesy Amount Read (CAR) or Intelligent Character Recognition (ICR) hardware. The number of encoding errors tracked that are attributed to CAR/ICR versus manual key payments and compare the error percentages for the two methods. 5. The number of lockbox customers, remittance documents, and checks (annually) that have been converted to image technology. 6. The number of wholesale and retail lockboxes for which FI provides data capture and tape/transmission output for each lockbox site proposed. Specify numbers by method of delivery. 7. Data consolidation for customers' multi-lockbox systems. 8. The earliest transmission time available to a customer without affecting the ability to deposit all checks received for a ledger credit day. 9. Management of data capture programming in the lockbox area, or managed from a centralized systems development department. If other than lockbox area, controls over the lockbox has on the work processed. 10. Procedures to ensure that transmissions are received successfully and contain all remittance payment detail. 11. Retention period for retrieval of remittance payment detail files.	

CATEGORY	CRITERIA	MAXIMUM POINTS - 50
DISASTER RECOVERY & CONTINUITY PLANS	1. Procedures established for disaster recovery for all existing lockboxes and branches and back-up sites. 2. Procedures for how lockbox depositary will maintain processing in case of a power outage lasting up to 48 hours. 3. Implementation of FI's disaster recovery plan if a disaster caused failure in operations for more than 48 hours. 4. Maintenance of processing lockbox payments with less than 100% equipment utilization for any length of time, i.e., continuation of 100% lockbox processing in the event of an equipment breakdown, power failure, or other circumstance that interrupts work/site operations. 5. Contractual agreements FI has with equipment manufacturers for additional equipment should a disaster occur for all areas of remittance processing, including mail extraction and image processing. 6. Procedures for use of a back-up postal facility for contingency situations at the Postal Service. 7. Establishment of a contingency (back-up) processing site in the event normal operations cease for more than 48 hours. 8. Employee training at branches, processing/contingency sites in anticipation of power outage, terrorist attack, bomb threat, earthquake, biochemical attack, fire, hurricane/tornado, etc. 9. Procedures for accounting for lockbox remittances that are shipped to another processing site. 10. Frequency of testing disaster recovery and continuity plans and revising procedures.	

CATEGORY	CRITERIA	MAXIMUM POINTS - 7 0
LOCKBOX PROCESSING	1. The lockbox department's processing flow/work flow. Highlight the quality control checkpoints and the components that are directly controlled by the lockbox manager. Include a schematic or flow chart of the processing procedures. 2. The controls in place to ensure accurate processing per agency specifications. 3. Priority handling of items for certain lockbox customers (e.g., large-dollar/item volume). 4. Peak processing periods and procedures to handle the increased volume. 5. Processing both retail, wholesale and specialized payments on the same equipment in the lockbox department and prioritizing those payments for processing. 6.Throughput capacity per day on all equipment, including the age of equipment and any plan to upgrade the equipment. 7. Back-up lockbox processing arrangements in the event of an automated equipment or system failure. 8. List financial institution's and lockbox department's holidays. 9. Use of third-party processors by financial institution, including couriers, for any part of this service. 10. Detecting and correcting out-of-balance problems. 11. Integration of return item processing with lockbox processing and length of time for agency notification once received by FI. 12. Handling unprocessable and exception items by FI. 13. Maintenance and disposition of coupons and other payment documents. 14. Recommended specifications for reply envelopes and remittance documents. 15. If bidding on retail applications, experience FI has managing this type of work.	

	16. If bidding on wholesale applications, experience FI has managing this type of work. 17. If bidding on specialized wholesale applications, experience FI has managing this type of work.	
CATEGORY	**CRITERIA**	**MAXIMUM POINTS - 20**
RECORD RETENTION	1. Retention of all forms of lockbox collection service documents or records within the scope of the IEI for the entire term of the IEI.	

APPENDIX 3

PRICING RESPONSE TEMPLATES

RETAIL LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page i of iii

TMA CODE	DESCRIPTION	VOLUME	PRICE
010000	Demand Deposit Account Maintenance	2	
010100	General Account Activity - Debit Posting	1	
010101	General Account Activity - Credit Posting	67	
010310	DDA Statement - Manual - Hard Copy	1	
010320	DDA Statement – Custom	1	
010400	Account Analysis - Automated – Maintenance	1	
010600	General Account Relationship Assistance – Inquiries/Request	1	
010610	General Account Relationship Assistance – Copies	1	
050010	Retail Lockbox Maintenance	14	
050012	Retail LBX Maintenance - P.O. Box Rental	7	
050200	Retail LBX Remit - Machine Readable Item - Matched (scans)	384,091	
050201	Retail Lockbox Remit - Machine Readable – Unmatched	243,331	
050202	Retail Lockbox Remit - Machine Readable – Multi	7,497	
050211	Retail Lockbox Detail Sorting - Functional/Divisional	1	
050212	Retail Lockbox Detail Sorting - Rough Sort	39,232	
050214	Retail Lockbox Detail Sorting – Fine Sort Alphanumeric	591	
05021A	Retail Lockbox Photocopy	661	
05021I	Retail Lockbox Hand Open Mail	7	
05021L	Retail Lockbox Delivery Preparation Charge	24	
05021P	Retail Lockbox Special Handling	453	
050221	Retail Lockbox Data Capture - MICR Line	479	
050222	Retail Lockbox Date Capture – OCR /Micr Line	499,395	
050223	Retail Lockbox Data Capture - Numeric Dual Entry	19,431	
050226	Retail Lockbox Data Capture – Alphanumeric Single Entry	111,171	
050234	Retail Lockbox Stop File Processing	1	
050238	Retail Lockbox Merchant Card Processing	5	
050239	Special Retail Lockbox Services – Returns	237,967	
05023A	Retail Lockbox Cash Payment Processing	18	
05023B	Retail Lockbox Non-Standard Processing	2,005	
05023C	Retail Lockbox Research	411	
050300	Lockbox Deposit	38	
050301	Lockbox Deposit - Ticket Preparation	37	
050309	Lockbox Batch Processing	206	
050310	Lockbox Deposit Reporting - Automated Total	4	
050311	Lockbox Deposit Reporting - Automated Detail	1	
050320	Lockbox Deposit Reporting - Manual – Total	1	
050321	Lockbox Deposit Report - Manual Detail	1	
050329	Lockbox Deposit Reporting - Wire Automated Fixed	1	
050331	Lockbox Deposit Report - Custom Output	1	
050400	Lockbox Information Delivery - Auto Maintenance	1	

RETAIL LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___

TMA CODE	DESCRIPTION	VOLUME	PRICE
050401	LBX Information Delivery - Automated – Transmission	30,999	
050403	LBX Information Delivery - Automated – Tape	1	
050405	LBX Information Delivery - Automated - CD ROM	1	
050409	LBX Information Delivery - Automated – Diskette	34	
050410	Lockbox Information Delivery - Manual Postage	118	
050412	LBX information Delivery – Manual Expedited Mail	97	
050413	LBX Information Delivery - Manual - Courier/Messenger	92	
050500	LBX Reject Items - Exception Handling	4	
050510	Lockbox Reject Items - Customer Specified Handling	2	
050520	LBX Reject Items - OCR/MICR Repair	17	
050530	LBX Reject Items – Unprocessable	134	
050600	Lockbox Document Storage – Retention	1,416	
059999	Undefined Lockbox services	9	
059999SAS	SAS 70 Audit	1	
059999PCCFARSM	Lockbox Services - Paper Check Conversion - Detail Sort - Rough Sort Manual		
059999PCCFAIS	Lockbox Services - Image Services per Document Scanned		
059999PCCFADCA	Lockbox Services - Data Captured – Alphanumeric		
059999PCCFADTM	Lockbox Services - Data Transmission – Maintenance		
059999PCCFASD	Lockbox Services - Safekeeping & Destruction		
059999PCCFANSPB	Lockbox Services - Non-Standard Processing – Balancing		
101099215/215B	Special Depository Service -Variable SF-215/215B	34	
1010995515	Special Depository Service -Variable SF-5515	6	
400699DR&C	Global Information Reporting-Deposit Reporting & Compiling	8	
05031Z	Lockbox Deposit Reporting - Automated – Bundled	15	
05032Z	Lockbox Deposit Reporting - Manual - Bundled	1	
100000	Branch Deposit	5	
100200	Check Deposit Processing	41	
100210	Encoded Checks - On-Us	20,811	
100212	Encoded Checks - Local Clearinghouse	10,046	
100213	Encoded Checks - Local Fed	42,925	
100214	Encoded Checks - Other Fed	395,205	
100215	Encoded Checks - Fed RCPC	7,300	
10021Z	Encoded Checks – Bundled	127,168	
100220	Unencoded Checks - On-Us	13	
100222	Unencoded Checks - Local Clearinghouse	33	
100223	Unencoded Checks - Local Fed	285	
100224	Unencoded Checks - Other Fed	744	
100225	Unencoded Checks - Fed RCPC	76	
100228	Check Encoding Surcharge	1	

RETAIL LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___

TMA CODE	DESCRIPTION	VOLUME	PRICE
10022Z	Unencoded Checks – Bundled	1	
100230	Checks Deposited - MICR Reject/Repair	227	
100299	Check Processing – Undefined	1	
100310	Non US Collection Item - US Dollar/Non-US Dollar Outgoing	47	
100400	Return Item Processing – Regular	630	
100401	Return Item Processing - Special Handling	26	
100402	Return Item Processing - Reclear Item	1,868	
100420	Return Item Notification – Manual	47	
100440	Return Item Notification – Custom	188	
100502	Deposit Adjustment Processing – Checks	17	
151351	Check Image Capture	31,926	
151353	Check Image – CD ROM	4	
350000	Funds Transfer System Maintenance	1	
350300	Incoming Fedwire Transfer	10	
350320	Incoming Book Transfer	1	
350412	Funds Transfer Advice - Manual - Debit/Credit	1	
350521	Drawdown Request - Fedwire Transfer	6	
350560	Funds Transfer Investigation	1	
359999	Undefined Wire and Other Funds Transfer Services	1	
400000	Domestic Info Maint - Terminal/Network - Previous Day – Summary	1	
400001	Domestic Info Maint - Terminal/Network - Previous Day – Detail	1	
400003	Domestic Info Maint - Terminal/Network - Intra Day – Summary	1	
400004	Domestic Info Maint - Terminal/Network -Intra Day – Detail	1	
400110	Domestic Information - Loading - High speed	8	
400224	Domestic Reporting - Terminal/Network - Intra Day – Detail	3	
40022Z	Deposit Reporting Bundled	12	
400822	Information Services Administration - Customer ID – Storage	3	
409999	Undefined Information Services	6	
40TTTT	Total Information Service Charge	7	

The volume figures provided in this template are for evaluation purposes only. The template volumes do not reflect projections for future business, nor are they intended to reflect actual current business activity. FIs submitting responses to this IEI expressly acknowledge, without recourse, that volumes short of the numbers provided in any template, in any region (or regions in the aggregate), during the term of the new GLN will not provide grounds for an upward price adjustment in any case at any time. Volumes of business and levels of compensation are not guaranteed.

WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page i of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
010000	Demand Deposit Account Maintenance	53	
010100	General Account Activity - Debit Posting	21	
010101	General Account Activity - Credit Posting	1,583	
010310	DDA Statement - Manual - Hard Copy	0	
010320	DDA Statement – Custom	12	
010400	Account Analysis - Automated – Maintenance	12	
010600	General Account Relationship Assistance - Inquiries/Request	32	
010610	General Account Relationship Assistance – Copies	2	
0107ZZ	Special General Account Services – Bundled	1	
050000	Wholesale Lockbox Maintenance	65	
050002	Wholesale Lockbox Maintenance-P.O. Box Rental	29	
050100	Wholesale LBX Remittance Processing (non-scans)	207,635	
050101	Wholesale LBX Remittance – Machine Readable Item – Matched	80	
050110	Wholesale Lockbox Detail Sort-Alpha	330	
050111	Wholesale Lockbox Detail Sort-Functional/Divisional	10,784	
050112	Wholesale LBX Document Handling - Rough Sort	489,105	
050113	Wholesale Lockbox Detail Sorting - Fine Sort Numeric	287	
050115	Wholesale Lockbox Document Matching	82,048	
050116	Wholesale LBX Document Notation	42,723	
050117	Wholesale Lockbox Stapling-Attach Document	39,035	
050119	Custom Lockbox Special Handling	328,456	
05011A	Wholesale LBX Photocopy	51,150	
05011B	Wholesale LBX Special Photocopy	38,961	
05011D	Wholesale Lockbox Date Stamping	8,368	
05011E	Wholesale Lockbox Return Envelope W/Remittance Assoc	17,926	
05011F	Wholesale Lockbox Return Envelope W/Remittance Unassociated	74,125	
05011G	Wholesale Lockbox Destroy Envelopes	29,884	
05011H	Wholesale Lockbox Flatten Invoice	70,443	
05011I	Wholesale LBX Hand Open Mail	111,858	
05011J	Wholesale Lockbox Special Stamping	57,444	
05011K	Wholesale Lockbox Reinsert Detail in Envelope	2,267	
05011L	Wholesale LBX Delivery Preparation Charge	1,476	
05011M	Wholesale Lockbox Correspondence	10,591	
05011N	Wholesale LBX Paid In Full Verification	37,675	
05011P	Wholesale LBX Special Handling (define each w/suffix)	5,878	
05011R	Wholesale LBX Image	104,475	
05011RCK	Wholesale LBX Image – Check		
05011RINV	Wholesale LBX Image – Invoice		
05011RDOC	Wholesale LBX Image – Document		
050120	Wholesale Lockbox Data Capture – Fixed Charge	73	
050121	Wholesale LBX Data Capture - MICR Line	14,910	

WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page ii of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
050122	Wholesale Lockbox Date Capture – OCR/MICR Line	814	
050124	Wholesale LBX Data Capture - Numeric Single Entry	315,525	
050125	Wholesale Lockbox Data Capture - Alphanumeric Dual Entry	23,397,726	
050126	Wholesale LBX Data Capture - Alphanumeric Single Entry	4,060,816	
050129	Wholesale Lockbox Data Capture – Automated	5,782	
050130	Wholesale LBX Early Release	2	
050131	Wholesale LBX Multiple Payees	372,851	
050133	Wholesale LBX Multiple Output Locations	3	
050134	Wholesale Lockbox Custom Detail Assembly	31,464	
050135	Wholesale LBX Stop File Processing	125	
050136	Wholesale LBX Custom Programming	34	
050137	Wholesale Lockbox Custom Programming	56	
05013A	Wholesale Lockbox Merchant Card Processing	871	
05013B	Wholesale LBX Cash Payment Processing	3	
05013F	Wholesale LBX Non Standard Processing	2,644	
050300	Lockbox Deposit	907	
050301	Lockbox Deposit- Ticket Preparation	868	
050309	Lockbox Batch Processing	4,903	
050310	Lockbox Deposit Reporting - Automated Total	84	
050311	Lockbox Deposit Reporting - Automated Detail	4	
050320	Lockbox Deposit Reporting - Manual – Total	7	
050321	Lockbox Deposit Report - Manual Detail	27	
050329	Lockbox Deposit Reporting - Wire Automated Fixed	12	
050331	Lockbox Deposit Report - Custom Output	23	
050400	Lockbox Information Delivery - Auto Maintenance	20	
050401	LBX Information Delivery – Automated – Transmission	736,232	
050403	LBX Information Delivery – Automated – Tape	6	
050405	LBX Information Delivery – Automated - CD ROM	8	
050409	LBX Information Delivery – Automated – Diskette	810	
050410	Lockbox Information Delivery - Manual Postage	2,808	
050412	LBX information Delivery – Manual Expedited Mail	2,304	
050413	LBX Information Delivery - Manual - Courier/Messenger	2,184	
050500	LBX Reject Items - Exception Handling	105	
050510	Lockbox Reject Items - Customer Specified Handling	42	
050520	LBX Reject Items - OCR/MICR Repair	410	
050530	LBX Reject Items – Unprocessable	3,187	
050600	Lockbox Document Storage – Retention	33,620	
059999	Undefined Lockbox services	217	
059999SAS	SAS 70 Audit		
059999PCCFARSM	Lockbox Services - Paper Check Conversion - Detail Sort - Rough Sort Manual		

WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page iii of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
059999PCCFAIS	Lockbox Services - Image Services per Document Scanned		
059999PCCFADCA	Lockbox Services - Data Captured – Alphanumeric		
059999PCCFADTM	Lockbox Services - Data Transmission – Maintenance		
059999PCCFASD	Lockbox Services - Safekeeping & Destruction		
059999PCCFANSPB	Lockbox Services - Non-Standard Processing – Balancing		
101099215/215B	Special Depository Service -Variable SF-215/215B	808	
1010995515	Special Depository Service -Variable SF-5515	153	
400699DR&C	Global Information Reporting-Deposit Reporting & Compiling	193	
05031Z	Lockbox Deposit Reporting - Automated – Bundled	362	
05032Z	Lockbox Deposit Reporting - Manual - Bundled	8	
050331	Lockbox Deposit Reporting - Custom Output	1	
100000	Branch Deposit	1	
100200	Check Deposit Processing	3	
100210	Encoded Checks - On-Us	1,561	
100212	Encoded Checks - Local Clearinghouse	753	
100213	Encoded Checks - Local Fed	3,219	
100214	Encoded Checks - Other Fed	29,640	
100215	Encoded Checks - Fed RCPC	547	
10021Z	Encoded Checks – Bundled	9,538	
100220	Unencoded Checks - On-Us	1	
100222	Unencoded Checks - Local Clearinghouse	2	
100223	Unencoded Checks - Local Fed	21	
100224	Unencoded Checks - Other Fed	56	
100225	Unencoded Checks - Fed RCPC	6	
100230	Checks Deposited - MICR Reject/Repair	17	
100310	Non US Collection Item - US Dollar/Non-US Dollar Outgoing	3	
100400	Return Item Processing – Regular	47	
100401	Return Item Processing - Special Handling	2	
100402	Return Item Processing - Reclear Item	140	
100420	Return Item Notification – Manual	4	
100440	Return Item Notification – Custom	14	
100502	Deposit Adjustment Processing – Checks	1	
151351	Check Image Capture	2,394	
151353	Check Image – CD ROM	1	
350000	Funds Transfer System Maintenance	17	
350103	Outgoing Fedwire Transfer - Automated-Freeform -Straight-Thru	1	
350300	Incoming Fedwire Transfer	227	
350320	Incoming Book Transfer	11	
350399	Incoming USD International Wire	1	
350411	Funds Transfer Advice - Manual – Credit	1	
350412	Funds Transfer Advice - Manual - Debit/Credit	10	

WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page iiii of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
350521	Drawdown Request - Fedwire Transfer	132	
350560	Funds Transfer Investigation	2	
350711	SWIFT Message - Incoming - Internal Transfer	1	
359999	Undefined Wire and Other Funds Transfer Services	9	
400000	Info Maint - Terminal/Network - Previous Day – Summary	16	
400001	Domestic Info Maint - Terminal/Network - Previous Day – Detail	26	
400003	Domestic Info Maint - Terminal/Network - Intra Day – Summary	6	
400004	Domestic Info Maint - Terminal/Network -Intra Day – Detail	24	
400110	Domestic Information - Loading - High speed	192	
400224	Domestic Reporting - Terminal/Network - Intra Day – Detail	71	
40022Z	Deposit Reporting Bundled	276	
400822	Information Services Administration - Customer ID – Storage	72	
401000	Information Services Software – Maintenance	1	
409999	Undefined Information Services	153	
40TTTT	Total Information Service Charge	174	

The volume figures provided in this template are for evaluation purposes only. The template volumes do not reflect projections for future business, nor are they intended to reflect actual current business activity. FIs submitting responses to this IEI expressly acknowledge, without recourse, that volumes short of the numbers provided in any template, in any region (or regions in the aggregate), during the term of the new GLN will not provide grounds for an upward price adjustment in any case at any time. Volumes of business and levels of compensation are not guaranteed.

SPECIALIZED WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 __ Region 5 ___ Page i of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
010000	Demand Deposit Account Maintenance	1	
010100	General Account Activity - Debit Posting	1	
010101	General Account Activity - Credit Posting	17	
010310	DDA Statement - Manual - Hard Copy	1	
010320	DDA Statement – Custom	1	
010400	Account Analysis - Automated – Maintenance	1	
010600	General Account Relationship Assistance - Inquiries/Request	1	
010610	General Account Relationship Assistance – Copies	1	
0107ZZ	Special General Account Services – Bundled	1	
050000	Wholesale Lockbox Maintenance	1	
050002	Wholesale Lockbox Maintenance-P.O. Box Rental	1	
050100	Wholesale LBX Remittance Processing (non-scans)	2,097	
050101	Wholesale LBX Remittance - Machine Readable Item – Matched	1	
050110	Wholesale Lockbox Detail Sort-Alpha	3	
050111	Wholesale Lockbox Detail Sort-Functional/Divisional	109	
050112	Wholesale LBX Document Handling - Rough Sort	4,941	
050113	Wholesale Lockbox Detail Sorting - Fine Sort Numeric	3	
050115	Wholesale Lockbox Document Matching	829	
050116	Wholesale LBX Document Notation	432	
050117	Wholesale Lockbox Stapling-Attach Document	394	
050119	Custom Lockbox Special Handling	3,318	
05011A	Wholesale LBX Photocopy	517	
05011B	Wholesale LBX Special Photocopy	394	
05011D	Wholesale Lockbox Date Stamping	85	
05011E	Wholesale Lockbox Return Envelope W/Remittance Assoc	181	
05011F	Wholesale Lockbox Return Envelope W/Remittance Unassociated	749	
05011G	Wholesale Lockbox Destroy Envelopes	302	
05011H	Wholesale Lockbox Flatten Invoice	712	
05011I	Wholesale LBX Hand Open Mail	1,130	
05011J	Wholesale Lockbox Special Stamping	580	
05011K	Wholesale Lockbox Reinsert Detail in Envelope	23	
05011L	Wholesale LBX Delivery Preparation Charge	15	
05011M	Wholesale Lockbox Correspondence	107	
05011N	Wholesale LBX Paid In Full Verification	381	
05011P	Wholesale LBX Special Handling (define each w/suffix)	59	
05011R	Wholesale LBX Image	1,055	
05011RCK	Wholesale LBX Image – Check	1	
05011RINV	Wholesale LBX Image – Invoice	1	
05011RDOC	Wholesale LBX Image – Document	1	
050120	Wholesale Lockbox Data Capture - Fixed Charge	1	

SPECIALIZED WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page ii of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
050121	Wholesale LBX Data Capture - MICR Line	151	
050122	Wholesale Lockbox Date Capture - OCR/MICR Line	8	
050124	Wholesale LBX Data Capture - Numeric Single Entry	3,187	
050125	Wholesale Lockbox Data Capture - Alphanumeric Dual Entry	236,341	
050126	Wholesale LBX Data Capture - Alphanumeric Single Entry	41,018	
050129	Wholesale Lockbox Data Capture – Automated	58	
050130	Wholesale LBX Early Release	1	
050131	Wholesale LBX Multiple Payees	3,729	
050133	Wholesale LBX Multiple Output Locations	1	
050134	Wholesale Lockbox Custom Detail Assembly	318	
050135	Wholesale LBX Stop File Processing	1	
050136	Wholesale LBX Custom Programming	1	
050137	Wholesale Lockbox Custom Programming	1	
05013A	Wholesale Lockbox Merchant Card Processing	9	
05013B	Wholesale LBX Cash Payment Processing	1	
05013F	Wholesale LBX Non Standard Processing	27	
05013FSTAMP	Wholesale LBX Non-Standard Processing - Spec Stamp	211,300	
05013FPASSPRT	Wholesale LBX Non-Standard Processing – Passport	110,683	
05013FPHOTO	Wholesale LBX Non-Standard Processing - Photo sizing	27,964	
050199	Special Wholesale Lockbox Services	5	
050300	Lockbox Deposit	10	
050301	Lockbox Deposit- Ticket Preparation	9	
050309	Lockbox Batch Processing	52	
050310	Lockbox Deposit Reporting - Automated Total	1	
050311	Lockbox Deposit Reporting - Automated Detail	1	
050320	Lockbox Deposit Reporting - Manual – Total	1	
050321	Lockbox Deposit Report - Manual Detail	1	
050329	Lockbox Deposit Reporting - Wire Automated Fixed	1	
050331	Lockbox Deposit Report - Custom Output	1	
050400	Lockbox Information Delivery - Auto Maintenance	1	
050401	LBX Information Delivery - Automated – Transmission	7,750	
050403	LBX Information Delivery - Automated – Tape	1	
050405	LBX Information Delivery - Automated - CD ROM	1	
050409	LBX Information Delivery - Automated – Diskette	8	
050410	Lockbox Information Delivery - Manual Postage	30	
050412	LBX information Delivery - Manual Expedited Mail	24	
050413	LBX Information Delivery - Manual - Courier/Messenger	23	
050500	LBX Reject Items - Exception Handling	1	
050510	Lockbox Reject Items - Customer Specified Handling	1	
050520	LBX Reject Items - OCR/MICR Repair	4	
050530	LBX Reject Items – Unprocessable	34	

SPECIALIZED WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page iii of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
050600	Lockbox Document Storage – Retention	354	
059999	Undefined Lockbox services	2	
059999SAS	SAS 70 Audit		
059999PCCFARSM	Lockbox Services - Paper Check Conversion - Detail Sort - Rough Sort Manual		
059999PCCFAIS	Lockbox Services - Image Services per Document Scanned		
059999PCCFADCA	Lockbox Services - Data Captured – Alphanumeric		
059999PCCFADTM	Lockbox Services - Data Transmission – Maintenance		
059999PCCFASD	Lockbox Services - Safekeeping & Destruction		
059999PCCFANSPB	Lockbox Services - Non-Standard Processing – Balancing		
101099215/215B	Special Depository Service -Variable SF-215/215B	9	
1010995515	Special Depository Service -Variable SF-5515	2	
400699DR&C	Global Information Reporting-Deposit Reporting & Compiling	2	
05031Z	Lockbox Deposit Reporting - Automated – Bundled	4	
05032Z	Lockbox Deposit Reporting - Manual - Bundled	1	
100000	Branch Deposit	1	
100200	Check Deposit Processing	7	
100210	Encoded Checks - On-Us	3,642	
100212	Encoded Checks - Local Clearinghouse	1,758	
100213	Encoded Checks - Local Fed	7,512	
100214	Encoded Checks - Other Fed	69,161	
100215	Encoded Checks - Fed RCPC	1,278	
10021Z	Encoded Checks – Bundled	22,255	
100220	Unencoded Checks - On-Us	2	
100222	Unencoded Checks - Local Clearinghouse	6	
100223	Unencoded Checks - Local Fed	50	
100224	Unencoded Checks - Other Fed	130	
100225	Unencoded Checks - Fed RCPC	13	
100228	Check Encoding Surcharge	1	
10022Z	Unencoded Checks – Bundled	1	
100230	Checks Deposited - MICR Reject/Repair	40	
100299	Check Processing – Undefined	1	
100310	Non US Collection Item - US Dollar/Non-US Dollar Outgoing	8	
100400	Return Item Processing – Regular	110	
100401	Return Item Processing - Special Handling	4	
100402	Return Item Processing - Reclear Item	327	
100420	Return Item Notification – Manual	8	
100440	Return Item Notification – Custom	33	
100502	Deposit Adjustment Processing – Checks	3	
151351	Check Image Capture	5,587	
151353	Check Image - CD ROM	1	

SPECIALIZED WHOLESALE LOCKBOX PRICING TEMPLATE

Check the Applicable Region for Which this Pricing Proposal Applies:

Region 1 ___ Region 2 ___ Region 3 ___ Region 4 ___ Region 5 ___ Page iiii of iiii

TMA CODE	DESCRIPTION	VOLUME	PRICE
350000	Funds Transfer System Maintenance	1	
350300	Incoming Fedwire Transfer	2	
350320	Incoming Book Transfer	1	
350521	Drawdown Request - Fedwire Transfer	1	
359999	Undefined Wire and Other Funds Transfer Services	1	
400000	Domestic Info Maint - Terminal/Network - Previous Day – Summary	1	
400001	Domestic Info Maint - Terminal/Network - Previous Day – Detail	1	
400004	Domestic Info Maint - Terminal/Network -Intra Day – Detail	1	
400110	Domestic Information - Loading - High speed	2	
400224	Domestic Reporting - Terminal/Network - Intra Day – Detail	1	
40022Z	Deposit Reporting Bundled	3	
400822	Information Services Administration - Customer ID – Storage	1	
409999	Undefined Information Services	2	
40TTTT	Total Information Service Charge	2	

The volume figures provided in this template are for evaluation purposes only. The template volumes do not reflect projections for future business, nor are they intended to reflect actual current business activity. FIs submitting responses to this IEI expressly acknowledge, without recourse, that volumes short of the numbers provided in any template, in any region (or regions in the aggregate), during the term of the new GLN will not provide grounds for an upward price adjustment in any case at any time. Volumes of business and levels of compensation are not guaranteed.

APPENDIX 4

GLOSSARY OF GENERAL LOCKBOX TERMS

GLOSSARY OF GENERAL LOCKBOX TERMS

Adjusted Earnings Credit Rate (AECR) – Or the Adjusted Analysis Earnings Rate (AAER). The rate used to calculate imputed earnings on Treasury Time Balances (TTB) and Demand Deposit Accounts (DDAs). FMS adjusts the Earnings Credit Rate (published as an annual rate) to a monthly rate and uses it to determine the imputed earnings on the TTB and on deposits held overnight in DDAs at the QLP.

Agency – An organizational unit of the U.S. Government or recognized agent thereof. For the purposes of this document, an agency is a Federal Government user of lockbox services.

Agency Location Code (ALC) – A unique four- or eight-digit number assigned by FMS to identify agency stations and offices on agency accounting reports and documents.

Audit Trail - Deposit information printed on the back of checks and payment documents.

Authorized Agency Official (AAO) – the official of a Federal Government agency authorized to act for and bind the Federal agency under a memorandum of understanding (MOU).

Authorized Bank Official (ABO) – the official of the FI authorized to act for and bind the FI under a Designation and Authorization of Financial Agent **(**DFA), memorandum of understanding (MOU), or similar agreement.

Authorized Treasury Official (ATO) – The Financial Management Service (FMS) official authorized to act for and bind the U.S. Treasury regarding U.S. Government lockbox collections. Currently, the ATO is the Director of the Cash Management Directorate, FMS, U.S. Department of the Treasury.

Automated Clearing House (ACH) - A batch processing, store-and-forward system used by FIs and the Federal Reserve to distribute electronic debit and credit entries to the accounts of FIs.

Automated Clearing House (ACH) File Cutoff – The time each banking day at which CA$HLINK II ceases to designate deposits reported by QLPs as ACH file items. The cutoff time is set at 8:00 p.m. Eastern time (ET) on Banking Day 1.

Availability – The percentage of 0-Day, 1-Day, and 2-Day funds, as assigned by the QLP, contained in Federal agency deposits.

Banking Day – The part of any business day on which an office of a bank is open to the public for carrying on substantially all of its banking functions.

Bank Management – The process of reporting the QLP's monthly service charges in a manner determined by FMS for compensation purposes. (See the Treasury Financial Manual, Volume V, Chapter 3000, and Section 3055 for specific details.)

Batch Range - Any groupings of more than one block. The QLP will determine batch size.

Block - A grouping of 100 documents or less, sequentially numbered 00 through 99.

Business Day – A calendar day other than a Saturday or Sunday or any days defined as a holiday in the Federal Reserve Holiday Schedule. The QLP will adhere to this business day definition unless stated otherwise in an MOU/SOW.

Candling - Process of using a light machine to scan envelopes prior to destruction to ensure that all contents have been removed.

CA$HLINK II – FMS system used by QLP to report agency deposits for credit to the Treasury's account. The system creates electronic funds transfers to move funds from the QLP to the Treasury's account at the Federal Reserve Bank of New York (FRBNY).

CA$HLINK Deposit Report – The funds and accounting information contained on the deposit report form for a given deposit date, as reported by each authorized depositary to CA$HLINK II.

Central Reporting System (CRS) - An FMS system that will enable Federal agencies to more effectively manage the financial transaction information resulting from FMS' collection processes. This effort will greatly improve the way government agencies collect, analyze, and redistribute financial transaction information.

Check Lister - A tape similar to a calculator tape that lists the sequence number and remittance amount processed with totals.

Check Truncation – If and when authorized by law, the process of removing an original paper check from the check collection or return process and sent to a recipient, in lieu of such original paper check. A substitute check or information relating to the original check (including data taken from the MICR line of the original check or an electronic image of the original check), whether with or without subsequent delivery of the original paper check.

CIRA (Central Image and Research Archive) - An online central repository for all Paper Check Conversion (PCC) electronic check images with associated financial information and other agency data that may be captured at the time of the transaction. This system allows agencies or QLPs to access check images as well as generate reports.

Classification Key – Key elements within remittance documents for use in reporting Governmentwide accounting data into CA$HLINK II.

Compensating Balance - A balance placed at a financial institution in the Treasury Time Balance account. Compensation is made through the imputed earnings on the investable balance using the earnings credit rate. The investable balance includes a Treasury Time Balance held by the QLP in a separate non-interest-bearing account expressly for this purpose and (where appropriate) collected balances from lockbox deposits.

**CA$HLINK Account Number (CAN) -** A unique three-digit number used by financial agents to identify their reporting location for CA$HLINK II collection deposit reporting purposes.

Cutoff Time – a predesignated time beyond which transactions presented or actions requested will be considered the next bank day's business.

Demand Deposit Account (DDA) - An account maintained by the Treasury at the QLP for crediting agencies for lockbox deposits.

Deposit Date - The banking day on which the QLP posts deposits to the Treasury's DDA for the agency, prepares SF 215 Deposit Tickets with the voucher date assigned, and reports the deposits into CA$HLINK II. On the deposit date, the QLP receives settlement for remittances transmitted electronically, i.e., via ACH or Fedwire.

Depositary Compensation Securities - Non-marketable securities issued by the U.S. Treasury to FAs as an investment vehicle that will be used for investing funds maintained in the Treasury time account. Compensation is made by means of the interest accrued on these securities, which is paid to the FA on a monthly basis.

Depositary or Designated Depositary - A bank or other financial institution that has been designated by FMS to receive monies for credit to Treasury.

Designation and Authorization of Financial Agent (DFA) - Upon selection as a QLP, an FI executes a DFA with FMS. The DFA designates the FI as a financial agent of the United States and details the legal requirements, relationships, and expectations of FMS with respect to the provision of general lockbox services.

Direct Payment - A payment to the FA reimbursing it directly for banking services it provided. This payment, either an ACH or Fed Wire transaction, is made on a monthly basis.

Document - Any printed form, notice, or document received at the lockbox processing site.

Document Locator Number (DLN) - A control number assigned to every document and check input through the remittance processing system. It is used to control, identify, and locate processed documents.

Earnings Credit Rate - Or the Analysis Earnings Rate (AER). The 3-month Treasury Bill Auction average (Investment) rate used to compute the imputed value on compensating balances, average daily immediately available funds, and average daily uncollected funds.

Expedite Funds - When FMS asks a QLP to expedite funds, all funds deposited shall be credited to Treasury's account for the Federal agency on the same day as deposit and transferred to Treasury's account at the FRB on the same day. To expedite funds means to accelerate the deposit from the day after deposit to the day of deposit as defined in the Treasury Financial Manual, Volume V, Chapter 3000, and Section 3050.

Federal Funds Rate (FFR) - The daily interest rate at which reserves are traded among commercial banks for overnight use. The daily effective FFR is applied to the principal amount of a funds transfer delay to determine the amount of interest assessed a QLP. The daily FFR is published in the Federal Reserve Statistical Release (H.15) weekly.

Financial Agent (FA) – An FA is a qualified Financial Institution that is designated an agent by and enters into an agreement with the Financial Management Service, as principal, to provide various types of essential banking services.

Financial Institution (FI) – An FI is any institution eligible under 31 CFR 202.2 to be designated by the Financial Management Service as a Financial Agent to provide various types of essential banking services.

Funds Transfer Date (also known as Transfer Date) - The calendar date funds are moved from the QLP to the Treasury's account at FRBNY. Unless specified otherwise by FMS, the transfer date for an Expedite account is the deposit date, and the transfer date for a Non-Expedite account is the business day following the deposit date.

Funds Transfer Delay - The difference in time between the agreed-upon funds transfer date and the actual funds transfer date, measured in whole days, from the QLP to the Treasury's account at the Federal Reserve.

Header Information - Information key-entered at the beginning of a block of documents that will be valid for the entire block of documents.

Imperfect Document - Remittance or document items that do not meet the criteria of a perfect document and require additional perfection or correction before depositing.

Internal Credit Tickets – An internal accounting document of a QLP that is prepared to represent a credit entry to the Treasury's DDA at the QLP.

Internal Debit Tickets – An internal accounting document of a QLP that is prepared to represent a debit entry to the Treasury's DDA at the QLP. These debits are the result of returned items or other adjustments.

Internet Matching - The process of matching a paper check received at a lockbox location with associated remittance information, such as completed forms, that has been submitted online at the Pay.gov Web site.

Investable Balance - The amount of dollars the QLP has available to invest. The Investable Balance consists of (1) the Investable TTB to be placed by FMS in a separate non-interest-bearing time deposit account with the QLP, and (2) the Treasury Average Daily Collected Balance (TADCB) in the DDA. The value derived by the QLP from the interest-free use of the Investable Balance over a sufficient period of time is used as the source of the QLP's compensation for providing required services.

Invitation for Expressions of Interest (IEI) - The solicitation document covering the process by which interested FIs may bid to become a QLP and containing the technical requirements and criteria that must be met for consideration.

Julian Date - A system of numbering the days of the year chronologically from 001 through 365 (or 366 on leap years) used as the 6^{th}, 7^{th}, and 8^{th} digits of the Document Locator Number.

Leap Year - During leap years, when making monthly calculations, the QLP should use 29 days for February. When making calendar year calculations during leap years, the QLP should use 366 days.

Lockbox (paper) - A post office box established by the QLP for the purpose of receiving paper-based payments to a Federal agency.

Lockbox Depositary - A QLP designated under 31 Code of Federal Regulations (CFR) Part 202 as a depositary and financial agent of the U.S. Government, which meets the qualifications set forth in the Treasury Financial Manual, Volume V, Chapter 3000, Section 3020 and which is authorized by FMS to perform financial services known as lockbox services for Federal Government agencies.

Lockbox Services - The term used herein to describe all categories of financial services provided by QLPs. Lockbox services include:

> **Basic Depositary Services** – those services that Federal agencies would receive through a Treasury General Account (TGA) at a commercial bank or the FRB.
>
> **Standard Lockbox Services** – those services necessary for a Federal agency to process remittance documents and update its internal accounts receivable system.
>
> **Ancillary Lockbox Services** – those services that go beyond Standard Lockbox Services, as determined by FMS, and do not necessarily accelerate deposit of funds to the Treasury. The agency will pay for Ancillary Lockbox Services as explained in I TFM Bulletin No. 94-07, Responsibility for Payment of Lockbox Account Costs.

Memorandum of Understanding (MOU) - A three-party agreement detailing the specific General Lockbox Services to be performed for a Federal agency by a QLP. The MOU is executed by the QLP, FMS, and the agency either upon a successful bid for business by the QLP, or upon appointment by FMS of the QLP to perform General Lockbox Services for a Federal agency.

Multiple Checks - Two or more remittances submitted along with one document.

Multiple Remittance Documents - Two or more vouchers or documents submitted for one check.

Non-Scannable Document - A document does not possess a perfect pre-printed machine-readable line of remittance information to apply to a remitter's account, i.e., reproduced, handwritten, or altered.

Paper Check Conversion - The process of converting a check into an ACH debit entry transaction when the check imager reads the bank account (MICR) information from the bottom of the check and stores an electronic image of the check. The bank account information is then compared against a database to verify that the account is in good standing.

Pay.gov - A Government-wide transaction portal managed by FMS that offers a suite of electronic financial services to assist Federal program agencies. Pay.gov's services rest on four cornerstones: collections, forms acceptance and direct billing, access control, and reporting.

Perfect Document - A document that does possess a perfect, pre-printed, machine-readable line of remittance information to apply to a remitter's account, i.e., is not reproduced, handwritten, or altered.

Product Code Category - A standard six-character designation (suffixes may be added) that represents a specific and defined product or service the QLP performs to support financial services for Federal agencies. The Treasury recognizes the codes published by the Association for Financial Professionals (AFP), formerly the Treasury Management Association.

Qualified Lockbox Provider (QLP) – A QLP is a designated Financial Agent that becomes a service provider within the General Lockbox Network. A QLP may bid on or be assigned business within the General Lockbox Network, depending on the availability and location of that business.

Received Date - The actual calendar date, including weekends, that documents and remittances are received at a lockbox (timeframe 12:00 a.m. – 11:59 .m.).

Redeposited Item - An item that cannot be collected by the QLP upon first presentment and is redeposited into the agency-specific Treasury DDA for second presentment and collection (see **Returned Item**).

Retail Lockbox – A remittance that includes a scannable document; generally high item volume/low dollar value flows.

Remittance Document Imaging - A digital electronic representation of a remittance document. This process eliminates forwarding paper copies of remittance documents to the agencies, which facilitates retrieval of document and payment information much faster. QLPs have the capability of sending files to the agencies on a daily basis.

Remittances - Any cash, check, draft, or money order drawn on and payable through FIs in the United States.

Reserve Ratio - The standard percentage of funds in DDA and TTB accounts that cannot be invested by the QLP due to Federal Reserve requirements. The reserve requirement ratio is determined by the FRB.

Returned Item - An item that cannot be collected by the QLP after two presentments and is returned to the agency for disposition (see **Redeposited Item**).

Scanline - A line of machine-readable information that is pre-printed on a document and systematically scanned for payment and entity information.

Scannable Documents - One that possesses the line of machine-readable information that a Federal agency prints on payment documents or documents.

Settlement Date - The date on which the QLPs or their correspondents are scheduled to be debited or credited by the Federal Reserve for the exchange of electronic entries through the ACH.

SF 215 Deposit Ticket (SF 215) - The Treasury form prepared by a QLP with totals of checks and other negotiable instruments to credit the Treasury's DDA at a QLP for a specific Federal agency (see **Voucher**).

SF 5515 Debit Voucher (SF 5515) - The Treasury form prepared by a QLP to debit the Treasury's DDA at a QLP for a specific Federal agency to offset the account for a deposit adjustment (for example, returned item) (see **Voucher**).

Specialized Lockbox - May have the characteristics of retail or wholesale lockbox; generally, the business rules that guide processing are more complex. Additional documents received, other than the remittance, may require review that is more detailed. There may also be higher physical and personnel security requirements required for specialized lockbox applications.

Split payment - A single check that is received for more than one document and/or more than one remitter.

Statement of Work (SOW) - A document detailing the lockbox processing requirements of a Federal agency.

Transaction Date - The date an agency uses to determine timeliness and calculate penalties and interest, if any, for delinquent payments. The transaction date is always in Julian form; it is the date remittances are received and/or processed by the QLP.

Treasury Average Daily Collected Balance (TADCB) - (Also known as Treasury Average Net Collected Balance) - Standard formula for all QLPs to use to calculate the amount of availability of funds compensation due on a monthly basis (see Treasury Financial Manual, Volume V, Chapter 3000, Section 3070.10). The Treasury Average Daily Collected Balance is calculated

using both the actual and guaranteed availability of funds percentages as prescribed in Section 3070.20.

Treasury Financial Manual - The manual issued by the Financial Management Service containing procedures to be observed by all FAs, Federal agencies, and FRBs with respect to payments, collections, central accounting, financial reporting, and other governmentwide fiscal responsibilities of the Department of the Treasury.

Treasury Time Balance (TTB) - The amount of funds Treasury has deposited with the QLP in a non-interest-bearing time account to compensate for financial services performed by a QLP. The TTB may also be referred to as the compensating balance.

Treasury Web Application Infrastructure (TWAI) – The distinct architecture that supports a Web-based platform for FMS' electronic applications for its core business processes, such as ASAP, GWA and future projects. The TWAI is supported by the FRBs and is designed to maintain a high level of security and flexibility for FMS and its clients.

Unprocessable - Any document, item, or correspondence that cannot be processed by the QLP.

Value of Funds (VOF) - The value of earnings on Funds Transfer Delays and Voucher Delays. VOF are assessments for not crediting or transferring funds to the Federal Government timely. The VOF method is the basis for calculating compensation adjustments (see Treasury Financial Manual, Volume V, Chapter 3000, and Section 3065).

Voucher– Any of the four following documents:

- SF 2l5 - Standard agency deposit ticket
- SF 2l5A - IRS deposit ticket
- SF 215B - U.S. Customs Service deposit ticket
- SF 5515 - Debit voucher

Voucher Confirmation - An SF 215, SF 215A/B, or SF 5515 voucher that is signed or stamped by an officer of the QLP "confirming" an increase or decrease in the Treasury's DDA balance.

Voucher Date - The banking day a QLP prepares a Deposit Ticket or Debit Voucher to effect a credit, debit, or adjustment to the Treasury's DDA for an agency. For returned items, the QLP shall use the date the returned item is received as the voucher date. For all other deposits, the QLP shall use the original agency deposit date as the voucher date.

Voucher Delay - The difference in time, measured in whole days, between the voucher date and the deposit date. The delay in reporting vouchers to CA$HLINK II) results in the delayed transfer of funds to Treasury. The voucher delay earnings are calculated according to the formula set forth in the Treasury Financial Manual, Volume V, Chapter 3000, and Section 3065.

Wholesale Lockbox – Remittances may or may not have a scannable; generally, there are one or more documents in addition to the remittance that require some form of data capture that require more manual handling. Often, more payers are corporate remitters.